Nicht f. d. Austausch

UNTERSUCHUNGEN ÜBER EINE VERMUTUNG VON W. BURNSIDE

INAUGURALDISSERTATION
ZUR ERLANGUNG DER DOKTORWÜRDE
GENEHMIGT VON DER
MATHEMATISCH-NATURWISSENSCHAFTLICHEN FAKULTÄT
DER FRIEDRICH-WILHELMS-UNIVERSITÄT
ZU BERLIN

VON

RUDOLF KOCHENDÖRFFER
AUS BERLIN-PANKOW

TAG DER MÜNDLICHEN PRÜFUNG: 9. DEZEMBER 1936
TAG DER PROMOTION: 20. APRIL 1937

DRUCK VON B. G. TEUBNER IN LEIPZIG

N 14

REFERENTEN:
PROFESSOR DR. E. SCHMIDT ·
PROFESSOR DR. L. BIEBERBACH

R. UNIV.
BIBLIOTHEEK
LEIDEN

Sonderabdruck aus den „Schriften des Mathematischen Seminars und des Instituts für angewandte Mathematik der Universität Berlin" / Band 3

Einleitung.

Von W. BURNSIDE stammt folgender Satz über Permutationsgruppen[1]):

Es sei p^γ eine von p verschiedene Potenz der Primzahl p. Enthält eine Permutationsgruppe $\mathfrak{G}$ des Grades p^γ einen Zyklus der Ordnung p^γ, so ist $\mathfrak{G}$ zweifach transitiv oder imprimitiv. Im letzteren Fall ist $\mathfrak{G}$ eine zusammengesetzte Gruppe.

Im Anschluß an diesen Satz spricht BURNSIDE die Vermutung aus, daß ein entsprechender Satz schon dann gilt, wenn man voraussetzt, daß $\mathfrak{G}$ an Stelle des Zyklus der Ordnung p^γ eine beliebige transitive Abelsche (also reguläre) Untergruppe $\mathfrak{H}$ der Ordnung p^γ enthält.

Herr SCHUR hat gezeigt, daß die Vermutung in dieser Allgemeinheit nicht richtig ist.[2]) Es lassen sich nämlich primitive Gruppen $\mathfrak{G}$ des Grades p^γ angeben, welche eine transitive Abelsche Untergruppe $\mathfrak{H}$ vom Typ $(p, p, \ldots, p)$ enthalten und nicht zweifach transitiv sind. Dagegen hat Herr SCHUR a. a. O. den BURNSIDEschen Satz auf solche Gruppen $\mathfrak{G}$ mit transitiver zyklischer Untergruppe $\mathfrak{H}$ ausgedehnt, deren Grad eine beliebige zusammengesetzte Zahl n ist. Als weitere Verallgemeinerung bewies Herr WIELANDT folgende Sätze[3]):

Enthält eine Permutationsgruppe $\mathfrak{G}$, deren Grad n keine Primzahl ist, eine transitive Abelsche Untergruppe $\mathfrak{H}$ des Grades n, von deren Sylowgruppen wenigstens eine zyklisch ist, so ist $\mathfrak{G}$ entweder zweifach transitiv oder imprimitiv.

Jede imprimitive Permutationsgruppe $\mathfrak{G}$, die eine transitive Abelsche Untergruppe $\mathfrak{H}$ desselben Grades enthält, ist zusammengesetzt.

In dieser Arbeit sollen hauptsächlich solche Gruppen des Grades p^γ untersucht werden, bei welchen die fragliche transitive Abelsche Untergruppe das direkte Produkt von zwei zyklischen Gruppen ist. Über diese Gruppen wird sich folgender Satz ergeben:

---

1) W. Burnside, *Theory of Groups of Finite Order*. 2. Aufl. (1911), S. 343.

2) I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*. Sitzungsber. d. Preuß. Akad. d. Wissensch. 1933, S. 598—623.

3) H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen*. Math. Ztschr. Bd. 40 (1935), S. 582—587.

Es sei p^γ eine von p verschiedene Potenz der Primzahl p. $\mathfrak{H}$ sei eine reguläre Abelsche Permutationsgruppe des Grades p^γ vom Typ (p^α, p^β).

I. *Sind die beiden Invarianten p^α und p^β von $\mathfrak{H}$ voneinander verschieden, so ist jede Permutationsgruppe $\mathfrak{G}$ des Grades p^γ, welche $\mathfrak{H}$ als Untergruppe enthält, zweifach transitiv oder imprimitiv.*

II. *Ist dagegen $p^\alpha = p^\beta$, so lassen sich, außer im Falle $p = 2$, $\alpha = \beta = 1$, stets primitive Permutationsgruppen $\mathfrak{G}$ des Grades p^γ angeben, welche $\mathfrak{H}$ als Untergruppe enthalten und nicht zweifach transitiv sind.*

Der Beweis wird unter Benutzung der von Herrn SCHUR entwickelten Hilfsmittel geführt. Diese werden, soweit sie hier Verwendung finden, in § 1 ohne Beweis zusammengestellt.

Kurz nachdem diese Arbeit der Berliner Universität als Dissertation eingereicht worden war, wurde der hier bewiesene Satz von Fräulein D. MANNING veröffentlicht.[4]) Der dort angegebene Beweis stützt sich auf die Theorie der Gruppencharaktere.

§ 1.

$\mathfrak{G}$ sei eine Permutationsgruppe der Ordnung g in den Vertauschungssymbolen $1, 2, \ldots, n$, welche eine transitive Abelsche Untergruppe $\mathfrak{H}$ desselben Grades enthält. $\mathfrak{H}$ muß dann bekanntlich eine reguläre Gruppe, d. h. von der Ordnung n sein:

$$\mathfrak{H} = H_1 + H_2 + \cdots + H_n.$$

An Stelle von $1, 2, \ldots, n$ führen wir die n Elemente von $\mathfrak{H}$ als neue Vertauschungssymbole der Gruppe $\mathfrak{G}$ ein, indem wir dem Symbol ν $(\nu = 1, 2, \ldots, n)$ dasjenige Element H_ν von $\mathfrak{H}$ zuordnen, welches 1 in ν überführt.

Jeder Permutation $G = \begin{pmatrix} \nu \\ \nu' \end{pmatrix}$ $(\nu = 1, 2, \ldots, n)$

von $\mathfrak{G}$ entspricht so eine Permutation

$$\begin{pmatrix} H_\nu \\ H_{\nu'} \end{pmatrix} \qquad (\nu = 1, 2, \ldots, n)$$

der Elemente von $\mathfrak{H}$, die wieder mit G bezeichnet werden soll. Die der Gruppe $\mathfrak{G}$ entsprechende Permutationsgruppe in den neuen

4) D. Manning, *On simply transitive groups with transitive Abelian subgroups of the same degree.* Transactions Am. Math. Soc. Vol. 40 (1936), S. 324—342.

Symbolen nennen wir wieder $\mathfrak{G}$. Setzen wir $H_{\nu'} = H_{\nu_G}$, so können wir die Permutation G auch in folgender Form schreiben:

$$G = \begin{pmatrix} H \\ H_G \end{pmatrix} \qquad (H = H_1, H_2, \ldots, H_n).$$

Ist insbesondere G ein Element von $\mathfrak{H}$, so wird

$$H_G = HG. \tag{1}$$

Der Permutation G ordnen wir wie üblich die Matrix

$$G^* = (e_{P_G Q^{-1}}) \qquad (P, Q = H_1, H_2, \ldots, H_n)$$

zu, wo e_R gleich 0 oder 1 zu setzen ist, je nachdem R das Einheitselement oder ein anderes Element von $\mathfrak{H}$ bedeutet.

Mit $\mathfrak{V}$ bezeichnen wir den Ring aller derjenigen Matrizen, welche mit allen g Matrizen G^* vertauschbar sind. Da eine Matrix V aus $\mathfrak{V}$ insbesondere auch mit den n Matrizen H_ν vertauschbar sein muß, so hat sie bekanntlich die Form

$$V = x_{H_1} H_1^* + x_{H_2} H_2^* + \cdots + x_{H_n} H_n^* \tag{2}$$

oder

$$V = (x_{P^{-1}Q}) \qquad (P, Q = H_1, H_2, \ldots, H_n).$$

Nun ist

$$G^* V G^{*-1} = \left(x_{P_G^{-1} Q_G}\right) \qquad (P, Q = H_1, H_2, \ldots, H_n).$$

Damit V mit allen g Matrizen G^* vertauschbar ist, ergeben sich daher für jedes Element G von $\mathfrak{G}$ und für je zwei Elemente P und Q von $\mathfrak{H}$ die Bedingungen

$$x_{P_G^{-1} Q_G} = x_{P^{-1}Q} \tag{3}$$

für die Koeffizienten der Matrix V. Umgekehrt liegt auch jede Matrix $(x_{P^{-1}Q})$, deren Koeffizienten den gn^2 Bedingungen (3) genügen, in dem Ring $\mathfrak{V}$.

Kommen in der allgemeinsten Lösung der Gleichungen (3) genau r voneinander verschiedene Zahlen x_H vor, so läßt sich jede Matrix aus $\mathfrak{V}$ in der Gestalt

$$V = x_1 K_1 + x_2 K_2 + \cdots + x_r K_r$$

schreiben, wobei jede der Matrizen K_ϱ eine Summe von wohlbestimmten voneinander verschiedenen Matrizen H_ν^* ist, derart, daß jede Matrix H_ν^* in genau einem K_ϱ als Summand auftritt. Die Matrizen K_ϱ werden als *primäre Matrizen* bezeichnet.

Da insbesondere stets die Einheitsmatrix E in $\mathfrak{V}$ enthalten ist, so können wir etwa $K_1 = E$ setzen. Man sieht leicht, daß immer $r \geqq 2$ sein muß; denn neben der Einheitsmatrix ist auch stets die Summe aller von E verschiedenen Matrizen H_ν^* in $\mathfrak{V}$ enthalten.

Eine Summe von voneinander verschiedenen primären Matrizen heißt *Hauptmatrix*.[5]) Hat man eine Matrix aus $\mathfrak{B}$ in der Gestalt (2) dargestellt, so ist die Summe derjenigen Matrizen H_ν^*, die mit dem gleichen Koeffizienten auftreten, eine Hauptmatrix.

Gehen wir von den Matrizen H_ν^* wieder zu den zugehörigen Elementen H_ν der Gruppe $\mathfrak{H}$ zurück, so wird durch die Gruppe $\mathfrak{G}$ eine Einteilung der Elemente der Gruppe $\mathfrak{H}$ in r paarweise elementefremde Komplexe definiert:

$$\mathfrak{H} = \mathfrak{K}_1 + \mathfrak{K}_2 + \cdots + \mathfrak{K}_r.$$

Diese Komplexe heißen *primäre Komplexe*. Eine Summe von voneinander verschiedenen primären Komplexen heißt *Hauptkomplex*.

Im folgenden ist die *Ringeigenschaft* der Matrizenmenge $\mathfrak{B}$ von Wichtigkeit. Sind K_ϱ und K_σ zwei Hauptmatrizen, so ist $K_\varrho K_\sigma$ ebenfalls in $\mathfrak{B}$ enthalten und hat daher die Form

$$K_\varrho K_\sigma = y_1 K_1 + y_2 K_2 + \cdots + y_r K_r,$$

wobei die y_τ nichtnegative ganze Zahlen sind. Diese Eigenschaft der Matrizen K_ϱ überträgt sich unmittelbar auf die zugehörigen Komplexe $\mathfrak{K}_\varrho$, wenn man Summe und Produkt von Komplexen aus Elementen von $\mathfrak{H}$ nicht nach den Regeln des FROBENIUSschen Komplexkalküls bildet, sondern auf die Vielfachheit achtet, in der die Gruppenelemente auftreten. (Man rechnet also wie in dem durch die Gruppe definierten Gruppenring.) Bei dieser Definition der Multiplikation zweier Komplexe läßt sich dann das Produkt der zu K_ϱ und K_σ gehörenden Hauptkomplexe $\mathfrak{K}_\varrho$ und $\mathfrak{K}_\sigma$ in folgender Form schreiben:

$$\mathfrak{K}_\varrho \mathfrak{K}_\sigma = y_1 \mathfrak{K}_1 + y_2 \mathfrak{K}_2 + \cdots + y_r \mathfrak{K}_r.$$

Alle Elemente von $\mathfrak{H}$, die in dem gleichen primären Komplex enthalten sind, müssen also insbesondere in jedem Produkt $\mathfrak{K}_\varrho \mathfrak{K}_\sigma$ in derselben Vielfachheit auftreten.

Über die primären Komplexe gilt eine Reihe wichtiger Sätze, für deren Beweise auf die oben genannte Arbeit des Herrn SCHUR verwiesen sei.[6])

Es sei $\mathfrak{G}_1$ diejenige Untergruppe von $\mathfrak{G}$, die das Einheitselement von $\mathfrak{H}$ — als Vertauschungssymbol aufgefaßt — ungeändert läßt.

---

5) Der einfacheren Ausdrucksweise wegen lassen wir zu, daß eine Hauptmatrix insbesondere auch eine einzelne primäre Matrix sein darf. Entsprechendes gilt für die unten definierten Hauptkomplexe.

6) Beim Studium der Schurschen Arbeit ist zu beachten, daß dort die primären Komplexe auch für nicht-Abelsche reguläre Gruppen $\mathfrak{H}$ definiert werden.

Dann lassen sich die primären Komplexe in folgender Weise charakterisieren[7]):

A. *Die von E verschiedenen primären Komplexe stimmen mit den Transitivitätssystemen überein, in welche die Elemente von $\mathfrak{H}$ bei den Permutationen der Gruppe $\mathfrak{G}$ zerfallen.*

Insbesondere ist also die Gruppe $\mathfrak{G}$ dann und nur dann zweifach transitiv, wenn es nur zwei primäre Komplexe gibt, nämlich E und die Summe aller von E verschiedenen Elemente von $\mathfrak{H}$.

Ein Komplex $\mathfrak{K}$ von Elementen der Gruppe $\mathfrak{H}$ heißt *singulär*, wenn die durch die Elemente von $\mathfrak{K}$ erzeugte Untergruppe von $\mathfrak{H}$ von E und $\mathfrak{H}$ verschieden ist. Dann gilt[8]):

B. *Dann und nur dann ist die Gruppe $\mathfrak{G}$ imprimitiv, wenn mindestens ein Hauptkomplex singulär ist.*

Es sei $$\mathfrak{K} = H_{\nu_1} + H_{\nu_2} + \cdots + H_{\nu_m}$$

ein Komplex von voneinander verschiedenen Elementen der Gruppe $\mathfrak{H}$ und l eine zu der Ordnung n von $\mathfrak{H}$ teilerfremde ganze Zahl. Dann sind die Elemente $H_{\nu_1}^l, H_{\nu_2}^l, \ldots, H_{\nu_m}^l$ wieder alle voneinander verschieden. Wir setzen

$$\mathfrak{K}^{(l)} = H_{\nu_1}^l + H_{\nu_2}^l + \cdots + H_{\nu_m}^l.$$

Es gilt der Satz[9]):

Ist $\mathfrak{K}$ ein primärer Komplex, so gilt das gleiche von $\mathfrak{K}^{(l)}$.

Es sei jetzt $\mathfrak{K}$ ein primärer Komplex. Sind $l_1, l_2, \ldots, l_t$ die $t = \varphi(n)$ zu n teilerfremden Zahlen der Reihe $1, 2, \ldots, n$, so brauchen die Komplexe

$$\mathfrak{K}^{(l_1)}, \mathfrak{K}^{(l_2)}, \ldots, \mathfrak{K}^{(l_t)} \tag{4}$$

nicht alle voneinander verschieden zu sein. Es mögen etwa die e Komplexe $\mathfrak{K}^{(r_1)}, \mathfrak{K}^{(r_2)}, \ldots, \mathfrak{K}^{(r_e)}$ mit $\mathfrak{K}$ übereinstimmen. (Offenbar sind zwei primäre Komplexe entweder elementefremd oder miteinander identisch.) Die Zahlen $r_1, r_2, \ldots, r_e$ bilden dann mod n (bei der Multiplikation) eine Untergruppe der Zahlen $l_1, l_2, \ldots, l_t$. Daher kommen in der Reihe (4) genau $f = \frac{t}{e}$ voneinander verschiedene Komplexe $\mathfrak{K}^{(s_1)}, \mathfrak{K}^{(s_2)}, \ldots, \mathfrak{K}^{(s_f)}$ vor, und jeder dieser Komplexe tritt e-mal auf. Die Summe

$$\mathfrak{S} = \mathfrak{K}^{(s_1)} + \mathfrak{K}^{(s_2)} + \cdots + \mathfrak{K}^{(s_f)}$$

heißt die *Spur* des Komplexes $\mathfrak{K}$.

---

7) Vgl. Schur, a. a. O. § 2.
8) Vgl. Schur, a. a. O. § 3.
9) Vgl. Schur, a. a. O. § 4.

Ein Komplex (der kein Hauptkomplex zu sein braucht) heißt *rational*, wenn er mit jedem Element H auch jede Potenz H^l mit einem zu n teilerfremden Exponenten l enthält.

Die Spur eines primären Komplexes ist immer ein rationaler Komplex.

§ 2.

$\mathfrak{H}$ sei eine reguläre Abelsche Permutationsgruppe der Ordnung p^γ vom Typ (p^α, p^β). Die beiden Invarianten p^α und p^β seien voneinander verschieden.

Die Elemente A und B mögen eine Basis von $\mathfrak{H}$ bilden, so daß sich jedes Element H auf eine und nur eine Weise in der Form

$$H = A^\varrho B^\sigma \qquad (\varrho = 0, 1, \ldots, p^\alpha - 1;\ \sigma = 0, 1, \ldots, p^\beta - 1)$$

darstellen läßt. Die Ordnung p^α von A sei größer als die Ordnung p^β von B.

Mit Hilfe der Basis A, B teilen wir die Elemente von $\mathfrak{H}$ in zwei Klassen $\mathfrak{W}$ und $\mathfrak{Z}$ ein, indem wir festsetzen, daß die Klasse $\mathfrak{W}$ aus allen denjenigen Elementen $A^a B^b$ besteht, bei welchen die Ordnung der $\mathfrak{A}$-Komponente A^a größer ist als die Ordnung der $\mathfrak{B}$-Komponente B^b. Die Klasse $\mathfrak{Z}$ enthalte alle übrigen Elemente von $\mathfrak{H}$. $p^\varkappa$ bzw. p^λ seien die höchsten Potenzen von p, welche in a bzw. b aufgehen, so daß $a = p^\varkappa c$, $b = p^\lambda d$, $(c, p) = (d, p) = 1$ gesetzt werden kann. Dann hat A^a die Ordnung $p^{\alpha-\varkappa}$, B^b die Ordnung $p^{\beta-\lambda}$. $A^a B^b$ gehört dann und nur dann zur Klasse $\mathfrak{W}$, wenn $\alpha - \varkappa > \beta - \lambda$ ist. Dies ist offenbar stets erfüllt, wenn $\varkappa = 0$ ist.

Die Elemente der Klasse $\mathfrak{W}$ teilen wir weiter in die beiden Klassen $\mathfrak{X}$ und $\mathfrak{Y}$ ein. Die Klasse $\mathfrak{X}$ bestehe dabei aus allen Elementen $A^a B^b$, bei welchen der Exponent a der $\mathfrak{A}$-Komponente zu p teilerfremd ist, während die Klasse $\mathfrak{Y}$ alle übrigen Elemente der Klasse $\mathfrak{W}$ enthält.

Schließlich fassen wir zu der Unterklasse $\mathfrak{X}(\lambda)$ von $\mathfrak{X}$ alle diejenigen Elemente $A^a B^b$ von $\mathfrak{X}$ zusammen, bei welchen der Exponent b der $\mathfrak{B}$-Komponente genau durch p^λ teilbar ist. Die entsprechenden Unterteilungen nehmen wir bei den Klassen $\mathfrak{Y}$ und $\mathfrak{Z}$ vor. Dann ist[10])

$$\mathfrak{X} = \mathfrak{X}(0) + \mathfrak{X}(1) + \cdots + \mathfrak{X}(\beta)$$
$$\mathfrak{Y} = \mathfrak{Y}(0) + \mathfrak{Y}(1) + \cdots + \mathfrak{Y}(\beta)$$
$$\mathfrak{Z} = \mathfrak{Z}(0) + \mathfrak{Z}(1) + \cdots + \mathfrak{Z}(\beta).$$

Für jede zu p teilerfremde Zahl l gehören offenbar $A^a B^b$ und $A^{la} B^{lb}$ der gleichen Klasse an. Jede der Klassen $\mathfrak{X}(0), \ldots, \mathfrak{X}(\beta)$,

10) Die hier aufgezählten Klassen können zum Teil leer sein.

$\mathfrak{Y}(0), \ldots, \mathfrak{Y}(\beta)$, $\mathfrak{Z}(0), \ldots, \mathfrak{Z}(\beta)$ ist daher als rationaler Komplex zu bezeichnen.

Ist H ein Element der Ordnung p^μ, so bezeichnen wir als *Spur* von H die Summe der $\varphi(p^\mu)$ Potenzen H^l mit einem zu p teilerfremden Exponenten aus der Reihe $1, 2, \ldots, p^\mu$. Die Spur eines Elementes nennen wir auch *Elementarspur*. Jede Elementarspur kann als die Spur jedes ihrer Elemente aufgefaßt werden.

Die Klasse $\mathfrak{X}(\lambda)$ enthält $\varphi(p^{\beta-\lambda})$ voneinander verschiedene Elementarspuren. Wir können diese als Spuren der Elemente AB^{dp^λ} $(d = 1, 2, \ldots, p^{\beta-\lambda}; (d, p) = 1)$ auffassen. Jede dieser Elementarspuren enthält $\varphi(p^\alpha)$ Elemente. Folglich enthält die Klasse $\mathfrak{X}$

$$\varphi(p^\alpha)\,(\varphi(p^\beta) + \varphi(p^{\beta-1}) + \cdots + 1) = (p^\alpha - p^{\alpha-1})\,p^\beta$$

Elemente.

Das Element A^aB^b gehört zur Klasse $\mathfrak{Z}(\lambda)$, wenn $\alpha - \varkappa \leqq \beta - \lambda$ ist. Die Ordnung von A^aB^b ist dann $p^{\beta-\lambda}$. Folglich enthält jede Elementarspur der Klasse $\mathfrak{Z}(\lambda)$ $\varphi(p^{\beta-\lambda})$ Elemente. In jeder Elementarspur ist genau ein Element der Form $A^{dp^\varkappa}B^{p^\lambda}$ enthalten. Bei einem festen Wert von $\varkappa$ kommen für d $\varphi(p^{\alpha-\varkappa})$ Werte in Betracht, nämlich die zu p teilerfremden Zahlen der Reihe $1, 2, \ldots, p^{\alpha-\varkappa}$. Dementsprechend gibt es für ein festes $\varkappa$ $\varphi(p^{\alpha-\varkappa})$ Elementarspuren in $\mathfrak{Z}(\lambda)$. Da $\alpha - \varkappa$ die Werte $0, 1, \ldots, \beta - \lambda$ annehmen darf, enthält $\mathfrak{Z}(\lambda)$ im ganzen

$$1 + \varphi(p) + \cdots + \varphi(p^{\beta-\lambda}) = p^{\beta-\lambda}$$

voneinander verschiedene Elementarspuren, also $\varphi(p^{\beta-\lambda})\,p^{\beta-\lambda}$ Elemente. In der ganzen Klasse $\mathfrak{Z}$ sind infolgedessen

$$\varphi(p^\beta)\,p^\beta + \varphi(p^{\beta-1})\,p^{\beta-1} + \cdots + 1 = \frac{p^{2\beta+1}+1}{p+1}$$

Elemente enthalten.

Die Klasse $\mathfrak{Y}$ enthält schließlich die übrigen

$$p^{\alpha+\beta} - (p^\alpha - p^{\alpha-1})\,p^\beta - \frac{p^{2\beta+1}+1}{p+1} = p^{\alpha+\beta-1} - \frac{p^{2\beta+1}+1}{p+1}$$

Elemente von $\mathfrak{H}$. Die Bedingungen für die Zugehörigkeit des Elementes A^aB^b zu der Klasse $\mathfrak{Y}(\lambda)$ lauten $\alpha - \varkappa > \beta - \lambda$, $\varkappa > 0$. Ist $\alpha > \beta + 1$, so gibt es für jeden Wert $\lambda = 0, 1, \ldots, \beta$ Zahlen $\varkappa$, welche diesen Ungleichungen genügen. Ist dagegen $\alpha = \beta + 1$, so läßt sich nur im Falle $\lambda = 0$ kein passendes $\varkappa$ finden. Daher sind im Falle $\alpha > \beta + 1$ in jeder der Klassen $\mathfrak{Y}(0), \mathfrak{Y}(1), \ldots, \mathfrak{Y}(\beta)$ Elemente enthalten, und für $\alpha = \beta + 1$ ist nur die Klasse $\mathfrak{Y}(0)$ leer.

Wir beweisen noch zwei Hilfssätze, die später gebraucht werden.

Unter der *Hauptspur* eines Elementes H der Ordnung p^μ verstehen wir die Summe aller $p^{\mu-1}$ Potenzen H^m mit denjenigen Exponenten m aus der Reihe $1, 2, \ldots, p^\mu$, welche der Kongruenz $m \equiv 1 \pmod{p}$ genügen.

$\mathfrak{U}$ sei die durch $A^{p^{\alpha-1}}$ erzeugte zyklische Untergruppe der Ordnung p von $\mathfrak{H}$.

Hilfssatz I: Es sei $W = A^a B^b$ ein Element der Klasse $\mathfrak{W}$. Ist die Ordnung von W größer als p, so besteht die Hauptspur $\mathfrak{w}$ von W aus vollen Nebengruppen nach $\mathfrak{U}$.

Beweis: Da die Hauptspur eines Elementes W' aus $\mathfrak{w}$ wieder $\mathfrak{w}$ ist, braucht offenbar nur bewiesen zu werden, daß für jede der Zahlen $q = 1, 2, \ldots, p-1$ $WA^{qp^{\alpha-1}}$ wieder in $\mathfrak{w}$ enthalten ist. Setzen wir wieder $a = cp^\varkappa$, $b = dp^\lambda$ mit $(c, p) = (d, p) = 1$, so ist wegen der Zugehörigkeit zur Klasse $\mathfrak{W}$ $\alpha - \varkappa > \beta - \lambda$. Folglich ist $B^{bp^{\alpha-\varkappa-1}} = E$. Bestimmen wir c' aus der Kongruenz $c'c \equiv 1 \pmod{p^\alpha}$, so wird

$$WA^{qp^{\alpha-1}} = A^{cp^\varkappa + qp^{\alpha-1}} B^b = A^{cp^\varkappa(1+c'qp^{\alpha-\varkappa-1})} B^b B^{bc'qp^{\alpha-\varkappa-1}} = W^{1+c'qp^{\alpha-\varkappa-1}}.$$

Da nun die Ordnung von W größer als p sein sollte, so ist $\alpha - \varkappa > 1$, d. h. $W^{1+c'qp^{\alpha-\varkappa-1}}$ ist in $\mathfrak{w}$ enthalten.

Es sei $\mathfrak{K}$ ein Komplex von voneinander verschiedenen Elementen der Gruppe $\mathfrak{H}$, welcher aus vollen Nebengruppen nach einer Untergruppe $\mathfrak{H}'$ von $\mathfrak{H}$ besteht. In der oben eingeführten Schreibweise ist mit $\mathfrak{K}^{(-1)}$ derjenige Komplex zu bezeichnen, welcher aus den inversen der in $\mathfrak{K}$ enthaltenen Elemente besteht.

Hilfssatz II: Enthält der Komplex $\mathfrak{K}$ k Elemente, so kommt in $\mathfrak{K}\mathfrak{K}^{(-1)}$ jedes Element von $\mathfrak{H}'$ in der Vielfachheit k vor.

Beweis: $\mathfrak{K}^{(-1)}$ besteht ebenso wie $\mathfrak{K}$ aus vollen Nebengruppen nach $\mathfrak{H}'$. Das gleiche gilt daher von $\mathfrak{K}\mathfrak{K}^{(-1)}$. Folglich tritt in $\mathfrak{K}\mathfrak{K}^{(-1)}$ jedes Element von $\mathfrak{H}'$ ebenso oft auf wie das Einheitselement. Dieses tritt aber genau k-mal auf.

Ist $\mathfrak{K}$ insbesondere ein rationaler Komplex, so ist $\mathfrak{K}^{(-1)} = \mathfrak{K}$. Daher tritt dann in $\mathfrak{K}^2$ jedes Element von $\mathfrak{H}'$ in der Vielfachheit k auf.

§ 3.

Nach den Sätzen A und B des § 1 ist der erste Teil des in der Einleitung genannten Satzes mit folgender Behauptung identisch:

Wird durch eine Gruppe $\mathfrak{G}$ eine Einteilung der Gruppe $\mathfrak{H}$ in mehr als zwei primäre Komplexe definiert, so ist mindestens einer davon singulär.

Wir führen den Beweis indirekt.

(5) $$\mathfrak{H} = \mathfrak{K}_1 + \mathfrak{K}_2 + \cdots + \mathfrak{K}_r$$

sei eine Einteilung von $\mathfrak{H}$ in mehr als zwei primäre Komplexe. Wir werden aus der Annahme, daß keiner dieser Komplexe singulär sei, einen Widerspruch herleiten.

Bezeichnen wir mit $\mathfrak{S}_\varrho$ die Spur des Komplexes $\mathfrak{K}_\varrho$ ($\varrho = 1, 2, \ldots, r$), so mögen in der Reihe $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_r$ t voneinander verschiedene Spuren vorkommen. Die Bezeichnung sei so gewählt, daß $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_t$ voneinander verschieden sind. Dann ist

$$\mathfrak{H} = \mathfrak{S}_1 + \mathfrak{S}_2 + \cdots + \mathfrak{S}_t$$

eine Einteilung der Gruppe $\mathfrak{H}$ in t rationale Hauptkomplexe. Da einer der Komplexe $\mathfrak{K}_\varrho$, etwa $\mathfrak{K}_1$, gleich dem Einheitselement E ist, so ist auch $\mathfrak{S}_1 = E$; daher ist stets $t \geqq 2$.

In diesem Paragraphen behandeln wir zunächst den Fall $t = 2$.

In diesem Falle haben also alle Komplexe

(6) $$\mathfrak{K}_2, \mathfrak{K}_3, \ldots, \mathfrak{K}_r$$

die gleiche Spur $\mathfrak{S}_2$, die aus allen von E verschiedenen Elementen von $\mathfrak{H}$ besteht.

Jeder Komplex $\mathfrak{K}$ dieser Reihe enthält insbesondere Elemente der durch $A^{p^{\alpha-1}}$ erzeugten zyklischen Untergruppe $\mathfrak{U}$ der Ordnung p, da andernfalls auch in seiner Spur $\mathfrak{S}_2$ keine derartigen Elemente vorkommen könnten. Für jede ganze Zahl z ist nun $\mathfrak{K}^{(zp+1)}$ wieder ein Komplex der Reihe (6). $\mathfrak{K}^{(zp+1)}$ enthält nun aber die gleichen Elemente aus $\mathfrak{U}$ wie $\mathfrak{K}$; denn diese haben die Ordnung p. Folglich ist $\mathfrak{K}^{(zp+1)} = \mathfrak{K}$. $\mathfrak{K}$ enthält also zu jedem seiner Elemente auch dessen Hauptspur. Ferner gibt es $d = r - 1$ Zahlen der Reihe $1, 2, \ldots, p-1$, etwa $w_1, w_2, \ldots, w_d$, so daß die Komplexe (6) folgende Gestalt haben: $\mathfrak{K}^{(w_1)}, \mathfrak{K}^{(w_2)}, \ldots, \mathfrak{K}^{(w_d)}$. d ist offenbar ein Teiler von $p - 1$.

Im Falle $p = 2$ ist unser Beweis schon geführt. Denn für jede ungerade Zahl u wäre dann $\mathfrak{K}^{(u)} = \mathfrak{K}$, d. h. $\mathfrak{K}$ wäre selbst ein rationaler Komplex, also gleich seiner Spur $\mathfrak{S}_2$. Dann kämen aber entgegen unserer Annahme in der Zerlegung (5) nur zwei primäre Komplexe vor.

Alle Elemente der Klasse $\mathfrak{W}$, mit Ausnahme der $p - 1$ Elemente $A^{kp^{\alpha-1}}$ ($k = 1, 2, \ldots, p-1$), haben die Eigenschaft, daß ihre Hauptspuren aus vollen Nebengruppen nach $\mathfrak{U}$ bestehen (Hilfssatz I). Wie sich in § 2 ergab, enthält die Klasse $\mathfrak{W}$ $p^{\alpha+\beta} - \frac{p^{2\beta+1}+1}{p+1}$ Elemente.

Folglich gibt es in der ganzen Gruppe $\mathfrak{H}$

$$N = p^{\alpha+\beta} - \frac{p^{2\beta+1}+1}{p+1} - (p-1) = p^{\alpha+\beta} - \frac{p^{2\beta+1}+p^2}{p+1}$$

Elemente, deren Hauptspuren aus vollen Nebengruppen nach $\mathfrak{U}$ bestehen. In dem Komplex $\mathfrak{K}$ gibt es daher einen Teilkomplex $\mathfrak{K}^*$ von $\frac{1}{d} N$ Elementen, welcher aus vollen Nebengruppen nach $\mathfrak{U}$ besteht. Setzen wir $\mathfrak{K} = \mathfrak{K}^* + \mathfrak{K}^{**}$, so wird $\mathfrak{K}^{(-1)} = \mathfrak{K}^{*(-1)} + \mathfrak{K}^{**(-1)}$. In $\mathfrak{K}\mathfrak{K}^{(-1)} = \mathfrak{K}^*\mathfrak{K}^{*(-1)} + \mathfrak{K}^*\mathfrak{K}^{**(-1)} + \mathfrak{K}^{**}\mathfrak{K}^{*(-1)} + \mathfrak{K}^{**}\mathfrak{K}^{**(-1)}$ kommt nach Hilfssatz II in dem Teilkomplex $\mathfrak{K}^*\mathfrak{K}^{*(-1)}$ jedes Element von $\mathfrak{U}$ in der Vielfachheit $\frac{1}{d} N$ vor. Andrerseits ist wegen der Ringeigenschaft der Komplexe $\mathfrak{K}_\varrho$

$$\mathfrak{K}\mathfrak{K}^{(-1)} = y_1\mathfrak{K}_1 + y_2\mathfrak{K}_2 + \cdots + y_r\mathfrak{K}_r.$$

Weil nun jeder der Komplexe $\mathfrak{K}_1, \mathfrak{K}_2, \ldots, \mathfrak{K}_r$ Elemente aus $\mathfrak{U}$ enthält, so müßte jeder Koeffizient $y_\varrho \geqq \frac{1}{d} N$ sein. In $\mathfrak{K}\mathfrak{K}^{(-1)}$ würde also jedes Element von $\mathfrak{H}$ mindestens in der Vielfachheit $\frac{1}{d} N$ auftreten. $\mathfrak{K}$ und $\mathfrak{K}^{(-1)}$ enthalten je $\frac{p^{\alpha+\beta}-1}{d}$ Elemente. Folglich wäre

$$\left(\frac{p^{\alpha+\beta}-1}{d}\right)^2 \geqq \frac{1}{d} N p^{\alpha+\beta}.$$

Daraus würde aber folgen

$$\left(\frac{p^{\alpha+\beta}-1}{d}\right)^2 > \frac{1}{d} N (p^{\alpha+\beta}-1)$$

oder $p^{\alpha+\beta}-1 > dN$ und daher

$$d < \frac{p^{\alpha+\beta}-1}{N} = q. \tag{7}$$

Wäre nun $q > 2$, so ergäben sich folgende Ungleichungen:

$$p^{\alpha+\beta} - 1 > 2p^{\alpha+\beta} - 2\frac{p^{2\beta+1}+p^2}{p+1},$$

$$-1 > p^{\alpha+\beta} - 2\frac{p^{2\beta+1}+p^{2\beta}}{p+1} = p^{2\beta}(p^{\alpha-\beta}-2).$$

Die letzte Ungleichung ist aber offenbar falsch. Daher ist $q \leqq 2$. Dann liefert aber Ungleichung (7) einen Widerspruch zu unserer Annahme, daß in der Zerlegung (5) mehr als zwei primäre Komplexe enthalten seien, d. h. daß $r - 1 = d \geqq 2$ sei.

§ 4.

Wir kommen jetzt zu dem Fall, daß in der im vorigen Paragraphen durch Übergang zu den Spuren erhaltenen Einteilung

$$\mathfrak{H} = \mathfrak{S}_1 + \mathfrak{S}_2 + \cdots + \mathfrak{S}_t \tag{8}$$

mehr als zwei rationale Komplexe auftreten.

Wir beschränken uns zunächst auf ungerade Primzahlen.

Jedes Produkt $\mathfrak{S}_\mu \mathfrak{S}_\nu$ ist ein Hauptkomplex und hat daher die Form

$$\mathfrak{S}_\mu \mathfrak{S}_\nu = u_1 \mathfrak{K}_1 + u_2 \mathfrak{K}_2 + \cdots + u_r \mathfrak{K}_r. \tag{9}$$

Ein Element P von $\mathfrak{H}$ möge in $\mathfrak{S}_\mu \mathfrak{S}_\nu$ u-mal auftreten. P läßt sich dann auf u verschiedene Arten als Produkt ST eines Elementes S aus $\mathfrak{S}_\mu$ und eines Elementes T aus $\mathfrak{S}_\nu$ darstellen. Für jede zu p teilerfremde Zahl l tritt dann aber P^l ebenfalls in der Vielfachheit u in $\mathfrak{S}_\mu \mathfrak{S}_\nu$ auf, nämlich in Form der Produkte $S^l T^l$. Daher kommen alle Elemente der Spur von P in $\mathfrak{S}_\mu \mathfrak{S}_\nu$ in gleicher Vielfachheit vor; $\mathfrak{S}_\mu \mathfrak{S}_\nu$ ist also ein rationaler Komplex. Folglich haben in (9) alle Komplexe $\mathfrak{K}_\varrho$, welche auf die gleiche Spur führen, den gleichen Koeffizienten. Man kann also setzen

$$\mathfrak{S}_\mu \mathfrak{S}_\nu = v_1 \mathfrak{S}_1 + v_2 \mathfrak{S}_2 + \cdots + v_t \mathfrak{S}_t.$$

D. h. die $\mathfrak{S}_\tau$ bilden einen Ring.

Insbesondere müssen also alle Elemente eines beliebigen Komplexes $\mathfrak{S}_\tau$ in jedem Produkt $\mathfrak{S}_\mu \mathfrak{S}_\nu$ in gleicher Vielfachheit auftreten.

Unter der Annahme, daß in (8) mehr als zwei rationale Komplexe auftreten, von denen keiner singulär ist, werden wir nun aber spezielle Elemente eines dieser Komplexe angeben können, welche in gewissen Quadraten $\mathfrak{S}_\mu^2$ in verschiedener Vielfachheit auftreten.

Unser Beweis verläuft in einer Reihe von Einzelschritten.

1. Wir können annehmen, daß die beiden Elemente A und $A^{p^{\alpha-1}}$ dem gleichen Komplex der Zerlegung (8) angehören. Denn da der Komplex $\mathfrak{S}$, in welchem $A^{p^{\alpha-1}}$ liegt, nicht singulär sein soll, so enthält er mindestens ein Element $A_1 = A^k B^m$ mit $(p, k) = 1$. Die Elemente A_1 und B bilden wieder eine Basis von $\mathfrak{H}$. Ferner ist $A_1^{p^{\alpha-1}} = A^{k p^{\alpha-1}}$, da die Ordnung p^β von B kleiner sein sollte als die Ordnung p^α von A. Jetzt liegen aber A_1 und $A_1^{k' p^{\alpha-1}}$ ($k' k \equiv 1 \bmod p^\alpha$) in $\mathfrak{S}$; als rationaler Komplex enthält $\mathfrak{S}$ dann aber auch $A_1^{p^{\alpha-1}}$. Hätte also die alte Basis A, B nicht die verlangte Eigenschaft gehabt, so hätten wir allen unseren Betrachtungen, insbesondere auch der Klasseneinteilung des § 2, von vornherein die Basis A_1, B zugrunde legen können.

2. Der Beweis der folgenden beiden Hilfssätze wird in § 5 nachgeholt.

$\mathfrak{L}(\lambda)$ sei ein rationaler Komplex, in welchem die Exponenten der $\mathfrak{B}$-Komponenten aller Elemente genau durch p^λ teilbar sind. $\mathfrak{L}(\lambda)$ möge ferner mindestens ein Element der Klasse $\mathfrak{K}(\lambda)$ enthalten. Die Vielfachheit, in der ein Element H in $\mathfrak{L}(\lambda)^2$ auftritt, soll mit $v(H)$ bezeichnet werden.

Hilfssatz IIIa. $\mathfrak{L}(\beta)$ enthalte das Element $A^{p^{\alpha-1}}$, aber nicht das Einheitselement. Es ist stets $v(A) \leqq v\left(A^{p^{\alpha-1}}\right)$. Das Gleichheitszeichen steht nur dann, wenn $\mathfrak{L}(\beta)$ bereits alle von E verschiedenen Potenzen von A enthält.

Bedeutet λ eine der Zahlen $0, 1, \ldots, \beta - 1$, so gilt für diese Komplexe $\mathfrak{L}(\lambda)$

Hilfssatz IIIb: Es ist stets $v(A) \leqq v\left(A^{p^{\alpha-1}}\right)$. Es ist nur dann $v(A) = v\left(A^{p^{\alpha-1}}\right)$, wenn $\mathfrak{L}(\lambda)$ die ganze Klasse $\mathfrak{K}(\lambda)$ enthält.

3. $\mathfrak{T}$ sei ein beliebiger von E verschiedener Komplex der Zerlegung (8). Da $\mathfrak{T}$ nicht singulär ist, so sind in $\mathfrak{T}$ Elemente der Klasse $\mathfrak{K}$ enthalten. Diese mögen den Unterklassen $\mathfrak{K}(\lambda_1), \mathfrak{K}(\lambda_2), \ldots, \mathfrak{K}(\lambda_h)$ angehören. $\mathfrak{K}^*(\lambda)$ sei der in $\mathfrak{T}$ enthaltene Teilkomplex der Klasse $\mathfrak{K}(\lambda)$. Ferner seien

$$\mathfrak{Y}^*(\lambda_1), \ldots, \mathfrak{Y}^*(\lambda_h), \mathfrak{Z}^*(\lambda_1), \ldots, \mathfrak{Z}^*(\lambda_h)$$

die in $\mathfrak{T}$ enthaltenen (möglicherweise leeren) Teilkomplexe der Klassen

$$\mathfrak{Y}(\lambda_1), \ldots, \mathfrak{Y}(\lambda_h), \mathfrak{Z}(\lambda_1), \ldots, \mathfrak{Z}(\lambda_h).$$

Setzen wir $$\mathfrak{L}(\lambda) = \mathfrak{K}^*(\lambda) + \mathfrak{Y}^*(\lambda) + \mathfrak{Z}^*(\lambda) \qquad (\lambda = 1, 2, \ldots, h),$$

so ist $$\mathfrak{T} = \mathfrak{L}(\lambda_1) + \mathfrak{L}(\lambda_2) + \cdots + \mathfrak{L}(\lambda_h) + \mathfrak{M},$$

wo $\mathfrak{M}$ entweder leer ist oder nur solche Elemente enthält, bei denen die Exponenten der $\mathfrak{A}$-Komponenten durch p teilbar und die höchsten Potenzen von p, die in den Exponenten der $\mathfrak{B}$-Komponenten aufgehen, von $p^{\lambda_1}, p^{\lambda_2}, \ldots, p^{\lambda_h}$ verschieden sind.

4. Potenzen von A können in $\mathfrak{T}^2$ offenbar nur in den Quadraten $\mathfrak{L}(\lambda_1)^2, \mathfrak{L}(\lambda_2)^2, \ldots, \mathfrak{L}(\lambda_h)^2, \mathfrak{M}^2$ auftreten, da sonst nur noch solche Elemente miteinander multipliziert werden, bei welchen die Exponenten der $\mathfrak{B}$-Komponenten durch verschieden hohe Potenzen von p teilbar sind, so daß die $\mathfrak{B}$-Komponente des Produkts von E verschieden ist. Ferner kann in $\mathfrak{M}^2$ das Element A nicht auftreten, da in $\mathfrak{M}$ die Exponenten der $\mathfrak{A}$-Komponenten aller Elemente durch p teilbar sind.

Da $\mathfrak{T}$ ein rationaler Komplex ist, so gilt das gleiche offenbar auch für jeden Teilkomplex $\mathfrak{L}(\lambda)$. Da $\mathfrak{L}(\lambda)$ außerdem Elemente der zugehörigen Klasse $\mathfrak{K}(\lambda)$ enthält, läßt sich Hilfssatz IIIb bzw. für $\lambda = \beta$ Hilfssatz IIIa anwenden. Daher ist zunächst in jedem Komplex $\mathfrak{L}(\lambda)^2$ die Vielfachheit von A nicht größer als die von $A^{p^{\alpha-1}}$. Da in $\mathfrak{T}^2$ aber A und $A^{p^{\alpha-1}}$ in gleicher Vielfachheit auftreten müssen, und da A in $\mathfrak{M}^2$ nicht enthalten ist, so muß schon in jedem einzelnen Komplex $\mathfrak{L}(\lambda)^2$ die Vielfachheit von A gleich der von $A^{p^{\alpha-1}}$ sein.

Aus Hilfssatz IIIb folgt dann für $\lambda < \beta$ weiter, daß in jedem Komplex $\mathfrak{L}(\lambda)$ bereits die ganze Klasse $\mathfrak{K}(\lambda)$ enthalten sein muß. Nach Hilfssatz IIIa muß überdies derjenige Komplex der Einteilung (8), welcher die beiden Elemente A und $A^{p^{\alpha-1}}$ enthält (in welchem also der Komplex $\mathfrak{L}(\beta)$ vorkommt), sämtliche von E verschiedenen Potenzen von A enthalten.

Folglich müssen in $\mathfrak{T}^2$ alle von E verschiedenen Potenzen von A in gleicher Vielfachheit auftreten.

Wir bemerken noch, daß in jedem Komplex $\mathfrak{L}(\lambda)^2$ die Vielfachheit von $A^{p^{\alpha-1}}$ größer ist als zwei; denn dies gilt nach Hilfssatz II (mit $\mathfrak{H}' = \mathfrak{U}$) schon für den Teilkomplex $\mathfrak{K}(\lambda)^2$.

5. Wir bezeichnen mit $\mathfrak{A}_p$ die durch das Element A^p erzeugte zyklische Gruppe der Ordnung $p^{\alpha-1}$. Man erkennt unmittelbar, daß jede Klasse $\mathfrak{K}(\lambda)$ aus vollen Nebengruppen nach $\mathfrak{A}_p$ besteht. Die Gesamtheit der von E verschiedenen Elemente von $\mathfrak{A}_p$ sei $\mathfrak{A}_p'$.

Wir zeigen, daß in jedem Komplex $\mathfrak{L}(\lambda)^2$ das Element A in keiner größeren Vielfachheit auftreten kann als irgendein Element aus $\mathfrak{A}_p'$.

Setzen wir $\mathfrak{Y}^*(\lambda) + \mathfrak{Z}^*(\lambda) = \mathfrak{R}^*(\lambda)$, so wird, da wir schon wissen, daß $\mathfrak{L}(\lambda)$ die ganze Klasse $\mathfrak{K}(\lambda)$ enthalten muß,

$$\mathfrak{L}(\lambda) = \mathfrak{K}(\lambda) + \mathfrak{R}^*(\lambda).$$

$\mathfrak{R}^*(\lambda)$ möge r^* Elemente enthalten. Diejenigen Elemente von $\mathfrak{K}(\lambda)$, bei denen der Exponent der $\mathfrak{A}$-Komponente die Form $zp + 1$ hat, bilden einen Teilkomplex $\mathfrak{K}'(\lambda)$. Wir setzen $\mathfrak{K}(\lambda) = \mathfrak{K}'(\lambda) + \mathfrak{K}''(\lambda)$. In $\mathfrak{K}'(\lambda)$ sind $p^{\alpha-1}\varphi(p^{\beta-\lambda})$, in $\mathfrak{K}''(\lambda)$ $p^{\alpha-1}(p-2)\varphi(p^{\beta-\lambda})$ Elemente enthalten. Es wird dann

$$\mathfrak{L}(\lambda)^2 = (\mathfrak{K}'(\lambda) + \mathfrak{K}''(\lambda))^2 + 2(\mathfrak{K}'(\lambda) + \mathfrak{K}''(\lambda))\mathfrak{R}^*(\lambda) + \mathfrak{R}^*(\lambda)^2.$$

Da der rationale Komplex $\mathfrak{K}(\lambda)$ aus vollen Nebengruppen nach $\mathfrak{A}_p$ besteht und $\varphi(p^\alpha)\varphi(p^{\beta-\lambda})$ Elemente enthält, so folgt aus Hilfssatz II, daß in $\mathfrak{K}(\lambda)^2$ jedes Element von $\mathfrak{A}_p$ in der Vielfachheit $\varphi(p^\alpha)\varphi(p^{\beta-\lambda})$ auftritt. Das Element A tritt in $\mathfrak{K}(\lambda)^2$ jedoch nur in dem Teilkomplex $\mathfrak{K}''(\lambda)^2$ auf, und zwar in der Vielfachheit $p^{\alpha-1}(p-2)\varphi(p^{\beta-\lambda})$. Da

in $\mathfrak{X}''(\lambda)\mathfrak{R}^*(\lambda)$ das Element A nicht vorkommt, so wird unsere Behauptung bewiesen sein, wenn wir gezeigt haben, daß in der Summe

$$2\,\mathfrak{X}'(\lambda)\mathfrak{R}^*(\lambda) + \mathfrak{R}^*(\lambda)^2 \tag{10}$$

die Vielfachheit von A um höchstens $p^{\alpha-1}\varphi(p^{\beta-\lambda})$ größer sein kann als die irgendeines Elementes von $\mathfrak{A}_p'$.

Dies ist sicher richtig, wenn $r^* \leqq \frac{1}{2}p^{\alpha-1}\varphi(p^{\beta-\lambda})$ ist; denn in (10) kommt A nur in $2\,\mathfrak{X}'(\lambda)\mathfrak{R}^*(\lambda)$ vor, und zwar in der Vielfachheit $2r^*$. Ist dagegen $r^* > \frac{1}{2}p^{\alpha-1}\varphi(p^{\beta-\lambda})$, etwa $2r^* = p^{\alpha-1}\varphi(p^{\beta-\lambda}) + e$, so tritt in (10) das Element A in der Vielfachheit $p^{\alpha-1}\varphi(p^{\beta-\lambda}) + e$ auf.

$\mathfrak{R}(\lambda) = \mathfrak{Y}(\lambda) + \mathfrak{Z}(\lambda)$ ist ein rationaler Komplex, welcher aus vollen Nebengruppen nach $\mathfrak{A}_p$ besteht. Wir setzen $\mathfrak{R}(\lambda) = \mathfrak{R}^*(\lambda) + \overline{\mathfrak{R}}(\lambda)$. Aus Hilfssatz II folgt, daß in

$$\mathfrak{R}(\lambda)^2 = \mathfrak{R}^*(\lambda)^2 + (\mathfrak{R}^*(\lambda) + \overline{\mathfrak{R}}(\lambda))\,\overline{\mathfrak{R}}(\lambda) + \mathfrak{R}^*(\lambda)\,\overline{\mathfrak{R}}(\lambda)$$

jedes Element von $\mathfrak{A}_p$ $p^{\alpha-1}\varphi(p^{\beta-\lambda})$-mal auftritt, da $\mathfrak{R}(\lambda)$ $p^{\alpha-1}\varphi(p^{\beta-\lambda})$ Elemente enthält. Weil nun aber $r^* > \frac{1}{2}p^{\alpha-1}\varphi(p^{\beta-\lambda})$ sein sollte, enthält $\overline{\mathfrak{R}}(\lambda)$ weniger Elemente als $\mathfrak{R}^*(\lambda)$, nämlich $p^{\alpha-1}\varphi(p^{\beta-\lambda}) - r^*$. Folglich kann in jedem der beiden Komplexe $(\mathfrak{R}^*(\lambda) + \mathfrak{R}(\lambda))\,\mathfrak{R}(\lambda)$ und $\mathfrak{R}^*(\lambda)\,\mathfrak{R}(\lambda)$ irgendein Element höchstens $(p^{\alpha-1}\varphi(p^{\beta-\lambda}) - r^*)$-mal auftreten. Daher muß in $\mathfrak{R}^*(\lambda)^2$ jedes Element aus $\mathfrak{A}_p$ in der Vielfachheit $p^{\alpha-1}\varphi(p^{\beta-\lambda}) - 2\,(p^{\alpha-1}\varphi(p^{\beta-\lambda}) - r^*) = e$ auftreten. Damit ist bewiesen, daß in (10) das Element A höchstens $p^{\alpha-1}\varphi(p^{\beta-\lambda})$-mal mehr auftreten kann als irgendein Element aus $\mathfrak{A}_p'$.

Da also A in jedem Komplex $\mathfrak{L}(\lambda)^2$ höchstens ebensooft auftreten kann wie irgendein Element aus $\mathfrak{A}_p'$, und da andrerseits in $\mathfrak{T}^2$ alle von E verschiedenen Potenzen von A in gleicher Vielfachheit vorkommen müssen, so folgt, daß in dem Komplex $\mathfrak{M}^2$ keine Potenz von A mehr auftreten darf. Denn die einzigen Potenzen von A, welche in $\mathfrak{M}^2$ vorkommen könnten, lägen in $\mathfrak{A}_p$.

6. Da alle Elemente der Klasse $\mathfrak{X}(0)$ bei der Einteilung (8) in dem gleichen Komplex enthalten sein müssen und da unserer Annahme gemäß in dieser Einteilung außer E noch mindestens zwei Komplexe vorkommen, so können wir jetzt unseren Komplex $\mathfrak{T}$ speziell so wählen, daß darin kein Element der Klasse $\mathfrak{X}(0)$ enthalten ist.

Damit dieser Komplex $\mathfrak{T}$ nicht singulär ist, muß es in $\mathfrak{M}$ einen Teilkomplex $\mathfrak{N}$ von solchen Elementen geben, bei denen die Exponenten der $\mathfrak{B}$-Komponenten nicht durch p teilbar sind. Da $\mathfrak{T}$ ein rationaler Komplex ist, so gilt das gleiche offenbar auch von $\mathfrak{N}$.

Wie wir erkannt haben, darf in $\mathfrak{M}^2$ keine Potenz von A auftreten. Das gleiche gilt dann aber auch von $\mathfrak{N}^2$. Daher darf $\mathfrak{N}$ keine Ele-

mentarspur der Klasse $\mathfrak{Y}(o)$ enthalten; denn in dem Quadrat derselben würde $A^{p^{\alpha-1}}$ auftreten (Hilfssatz I und II). Alle Elemente von $\mathfrak{N}$ liegen daher in $\mathfrak{Z}(o)$.

Weiter erkennt man, daß $\mathfrak{N}$ nur eine einzige Elementarspur enthalten darf. Wären nämlich zwei Elementarspuren $\mathfrak{z}_1$ und $\mathfrak{z}_2$ in $\mathfrak{N}$ enthalten, so gäbe es zu jedem Element $A^{pl}B^m$ aus $\mathfrak{z}_1$ wegen $(m, p) = 1$ ein Element $A^{pl_1}B^{-m}$ in $\mathfrak{z}_2$. Das Produkt dieser beiden Elemente würde aber eine Potenz von A in $\mathfrak{N}^2$ ergeben. Diese Potenz ist von E verschieden, da das Inverse eines Elementes aus $\mathfrak{z}_1$ wieder in $\mathfrak{z}_1$ enthalten ist.

Jede Elementarspur aus $\mathfrak{Z}(o)$ enthält $\varphi(p^\beta)$ Elemente. $\mathfrak{T}$ enthält also nur $\varphi(p^\beta)$ Elemente, bei denen die Exponenten der $\mathfrak{B}$-Komponenten nicht durch p teilbar sind. Folglich können in $\mathfrak{T}^2$ nur $2\varphi(p^\beta)$ derartige Elemente auftreten.

Nun ist aber auch derjenige Komplex der Zerlegung (8), dem A und $A^{p^{\alpha-1}}$ angehören, nicht singulär. Folglich enthält er mindestens $\varphi(p^\beta)$ Elemente, bei denen die Exponenten der $\mathfrak{B}$-Komponenten nicht durch p teilbar sind, denn er enthält mindestens ein solches Element und als rationaler Komplex auch dessen Spur. Daraus folgt aber, daß in $\mathfrak{T}^2$ jedes Element dieses Komplexes höchstens zweimal auftreten darf.

Insbesondere würde dies auch für $A^{p^{\alpha-1}}$ gelten. Damit haben wir jedoch einen Widerspruch erhalten; denn wir hatten in Punkt 4 unseres Beweises erkannt, daß $A^{p^{\alpha-1}}$ in $\mathfrak{T}^2$ stets in größerer Vielfachheit auftritt.

Für eine ungerade Primzahl hat sich also die Annahme, daß in der Zerlegung (8) mehr als zwei Komplexe vorkommen, als unzulässig erwiesen. In diesem Falle ist daher der erste Teil unseres Satzes bewiesen.

§ 5.

Beweis von Hilfssatz IIIa: Da $\mathfrak{L}(\beta)$ ein rationaler Komplex sein sollte und mindestens ein Element der Klasse $\mathfrak{X}(\beta)$ enthält, d. h. mindestens eine Potenz von A mit einem zu p teilerfremden Exponenten, so sind darin schon alle derartigen Potenzen von A enthalten, d. h. die ganze Klasse $\mathfrak{X}(\beta)$. Außerdem enthält $\mathfrak{L}(\beta)$ die Spur des Elementes $A^{p^{\alpha-1}}$, das ist die Gesamtheit $\mathfrak{U}'$ der von E verschiedenen Elemente der Untergruppe $\mathfrak{U}$. Ist $\alpha = 2$, so enthält damit $\mathfrak{L}(\beta)$ schon alle von E verschiedenen Potenzen von A. Ist aber $\alpha > 2$, so kann es in $\mathfrak{L}(\beta)$ noch einen weiteren Komplex $\mathfrak{Y}^*(\beta)$ von y^* Elementen der Klasse $\mathfrak{Y}(\beta)$ geben. Es ist $y^* \leqq p^{\alpha-1} - p$; denn die

Klasse $\mathfrak{Y}(\beta)$ umfaßt neben den Elementen von $\mathfrak{U}'$ sämtliche von E verschiedenen Potenzen von A mit einem durch p teilbaren Exponenten. Es wird dann

$$\mathfrak{L}(\beta) = \mathfrak{X}(\beta) + \mathfrak{Y}^*(\beta) + \mathfrak{U}'.$$

In $\mathfrak{L}(\beta)^2$ tritt $A^{p^{\alpha-1}}$ auf in den Komplexen

$$\mathfrak{X}(\beta)^2,\ \mathfrak{Y}^*(\beta)^2,\ \mathfrak{U}'^2,$$

und zwar der Reihe nach in der Vielfachheit

$$p^{\alpha-1}(p-1),\ y^*,\ p-2.$$

Da nämlich $\mathfrak{L}(\beta)$ ein rationaler Komplex sein sollte, so haben $\mathfrak{X}(\beta)$ und $\mathfrak{Y}^*(\beta)$ die gleiche Eigenschaft. Jeder der beiden Komplexe ist daher eine Summe von Elementarspuren, von denen sich wieder jede als Summe von elementaren Hauptspuren auffassen läßt und daher nach Hilfssatz I aus vollen Nebengruppen nach $\mathfrak{U}$ besteht. Folglich kann man auf $\mathfrak{X}(\beta)$ und $\mathfrak{Y}^*(\beta)$ Hilfssatz II anwenden. Daß in $\mathfrak{U}'^2$ $A^{p^{\alpha-1}}$ in der Vielfachheit $p-2$ auftritt, ist unmittelbar ersichtlich. Es wird also

$$v\left(A^{p^{\alpha-1}}\right) = p^{\alpha-1}(p-1) + y^* + p - 2.$$

A kann in $\mathfrak{L}(\beta)^2$ nur in $\mathfrak{X}(\beta)^2$ und $2\,\mathfrak{X}(\beta)\,(\mathfrak{Y}^*(\beta) + \mathfrak{U}')$ auftreten. Zu einem Element A^k aus $\mathfrak{X}(\beta)$ liegt das Element A^{-k+1} dann und nur dann ebenfalls wieder in $\mathfrak{X}(\beta)$, wenn $k \not\equiv 1 \pmod{p}$ ist. Die Anzahl $p^{\alpha-1}(p-2)$ solcher Elemente ist daher gleich der Vielfachheit von A in $\mathfrak{X}(\beta)^2$. In $\mathfrak{X}(\beta)\,(\mathfrak{Y}^*(\beta) + \mathfrak{U}')$ ist, wie man leicht erkennt, die Vielfachheit von A genau $y^* + p - 1$. Folglich wird

$$v(A) = p^{\alpha-1}(p-2) + 2y^* + 2p - 2.$$

Die Differenz $\quad v\left(A^{p^{\alpha-1}}\right) - v(A) = p^{\alpha-1} - p - y^*$

ist positiv, außer wenn $y^* = p^{\alpha-1} - p$ ist. Damit ist Hilfssatz III a bewiesen.

Beweis von Hilfssatz III b: 1. Die Elemente von $\mathfrak{L}(\lambda)$ fassen wir gemäß ihrer Zugehörigkeit zu den Klassen $\mathfrak{X}(\lambda)$, $\mathfrak{Y}(\lambda)$, $\mathfrak{Z}(\lambda)$ zu den Teilkomplexen $\mathfrak{X}^*(\lambda)$, $\mathfrak{Y}^*(\lambda)$, $\mathfrak{Z}^*(\lambda)$ zusammen:

$$\mathfrak{L}(\lambda) = \mathfrak{X}^*(\lambda) + \mathfrak{Y}^*(\lambda) + \mathfrak{Z}^*(\lambda).$$

Diese Teilkomplexe mögen x^*, y^* bzw. z^* Elemente enthalten. In $\mathfrak{X}^*(\lambda)$ seien u voneinander verschiedene Elementarspuren $\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_u$ enthalten. Nach § 2 ist $u \leqq \varphi(p^{\lambda-\lambda})$. Jede Elementarspur enthält $\varphi(p^\alpha)$ Elemente. Die Gesamtheit derjenigen $p^{\alpha-1}$ Elemente einer Ele-

mentarspur $\mathfrak{x}_\nu$, bei welchen der Exponent der $\mathfrak{A}$-Komponente die Form $kp+1$ hat, bezeichnen wir mit $\mathfrak{x}_\nu'$ und setzen $\mathfrak{x}_\nu = \mathfrak{x}_\nu' + \mathfrak{x}_\nu''$. Ferner sei

$$\mathfrak{X}'(\lambda) = \mathfrak{x}_1' + \mathfrak{x}_2' + \cdots + \mathfrak{x}_u',$$
$$\mathfrak{X}''(\lambda) = \mathfrak{x}_1'' + \mathfrak{x}_2'' + \cdots + \mathfrak{x}_u''.$$

Jeder der drei Teilkomplexe $\mathfrak{X}^*(\lambda)$, $\mathfrak{Y}^*(\lambda)$ und $\mathfrak{Z}^*(\lambda)$ ist rational. Nach den Hilfssätzen I und II wird daher insbesondere in $\mathfrak{X}^*(\lambda)^2$ $A^{p^{\alpha-1}}$ in der Vielfachheit $x^* = up^{\alpha-1}(p-1)$ auftreten. In

$$\mathfrak{X}^*(\lambda)^2 = \mathfrak{X}'(\lambda)^2 + 2\,\mathfrak{X}'(\lambda)\,\mathfrak{X}''(\lambda) + \mathfrak{X}''(\lambda)^2$$

kann A dagegen nur in dem Komplex $\mathfrak{X}''(\lambda)^2$ vorkommen, und zwar höchstens in der Vielfachheit $up^{\alpha-1}(p-2)$, da $\mathfrak{X}''(\lambda)$ nur $up^{\alpha-1}(p-2)$ Elemente enthält.

Unser Satz wird daher bewiesen sein, wenn wir gezeigt haben, daß in der Summe

$$(11)\quad 2\,\mathfrak{X}^*(\lambda)\,\mathfrak{Y}^*(\lambda) + 2\,\mathfrak{X}^*(\lambda)\,\mathfrak{Z}^*(\lambda) + \mathfrak{Y}^*(\lambda)^2 + \mathfrak{Z}^*(\lambda)^2 + 2\,\mathfrak{Y}^*(\lambda)\,\mathfrak{Z}^*(\lambda)$$

die Vielfachheit von A höchstens um $up^{\alpha-1}$ größer sein kann als die von $A^{p^{\alpha-1}}$, und zwar um genau $up^{\alpha-1}$ größer nur dann, wenn $u = \varphi(p^{\beta-\lambda})$ ist, d. h. wenn $\mathfrak{X}^*(\lambda) = \mathfrak{X}(\lambda)$ ist.

2. In dem Produkt $\mathfrak{Y}^*(\lambda)\,\mathfrak{Z}^*(\lambda)$ kann das Element A nicht auftreten, da bei allen Elementen dieses Produktes die Exponenten der $\mathfrak{A}$-Komponenten durch p teilbar sind. In den beiden Produkten $\mathfrak{X}^*(\lambda)\,\mathfrak{Y}^*(\lambda)$ und $\mathfrak{X}^*(\lambda)\,\mathfrak{Z}^*(\lambda)$ kann das Element A nur dadurch entstehen, daß ein solches Element aus $\mathfrak{X}^*(\lambda)$ mit einem Element aus $\mathfrak{Y}^*(\lambda)$ bzw. $\mathfrak{Z}^*(\lambda)$ multipliziert wird, bei welchem der Exponent der $\mathfrak{A}$-Komponente die Form $kp+1$ hat. Die Vielfachheit von A in (11) wird daher nicht verkleinert, wenn wir darin $\mathfrak{X}^*(\lambda)$ durch $\mathfrak{X}'(\lambda)$ ersetzen und $2\,\mathfrak{Y}^*(\lambda)\,\mathfrak{Z}^*(\lambda)$ fortlassen.

Ist S ein Element aus $\mathfrak{x}_\nu'$, so liegt $S^{-1}A$ in $\mathfrak{Y}(\lambda)$ oder $\mathfrak{Z}(\lambda)$. $\mathfrak{x}_\nu^{(\mathfrak{Y})}$ bzw. $\mathfrak{x}_\nu^{(\mathfrak{Z})}$ mögen aus denjenigen Elementen S von $\mathfrak{x}_\nu'$ bestehen, für welche $S^{-1}A$ in $\mathfrak{Y}(\lambda)$ bzw. in $\mathfrak{Z}(\lambda)$ liegt. Es genügt also, an Stelle von (11) die folgende Summe zu betrachten:

$$(12)\quad 2(\mathfrak{x}_1^{(\mathfrak{Y})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Y})})\,\mathfrak{Y}^*(\lambda) + \mathfrak{Y}^*(\lambda)^2 + 2(\mathfrak{x}_1^{(\mathfrak{Z})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Z})})\,\mathfrak{Z}^*(\lambda) + \mathfrak{Z}^*(\lambda)^2.$$

Bezeichnen wir mit $x^{(\mathfrak{Y})}$ die Anzahl der Elemente von $\mathfrak{x}_1^{(\mathfrak{Y})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Y})}$, mit $x^{(\mathfrak{Z})}$ die von $\mathfrak{x}_1^{(\mathfrak{Z})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Z})}$, so gilt $x^{(\mathfrak{Y})} + x^{(\mathfrak{Z})} = up^{\alpha-1}$.

3. $\mathfrak{Y}^*(\lambda)$ ist ein rationaler Komplex, der nach Hilfssatz I aus vollen Nebengruppen nach $\mathfrak{U}$ besteht. Aus Hilfssatz II folgt, daß in $\mathfrak{Y}^*(\lambda)^2$ $A^{p^{\alpha-1}}$ in der Vielfachheit y^* auftritt. In $2(\mathfrak{x}_1^{(\mathfrak{Y})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Y})})\,\mathfrak{Y}^*(\lambda)$

ist die Vielfachheit von A höchstens gleich der kleineren der beiden Zahlen $2x^{(\mathfrak{P})}$ und $2y^*$. Daher ist in

$$2(\mathfrak{x}_1^{(\mathfrak{P})} + \cdots + \mathfrak{x}_u^{(\mathfrak{P})})\,\mathfrak{P}^*(\lambda) + \mathfrak{P}^*(\lambda)^2 \tag{13}$$

die Vielfachheit von A um höchstens $x^{(\mathfrak{P})}$ größer als die von $A^{p^{\alpha-1}}$. Damit in (11) die Vielfachheit von A um $x^{(\mathfrak{P})} + x^{(\mathfrak{Z})}$ größer wird als die von $A^{p^{\alpha-1}}$, ist daher notwendig, daß in

$$2(\mathfrak{x}_1^{(\mathfrak{Z})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Z})})\,\mathfrak{Z}^*(\lambda) + \mathfrak{Z}^*(\lambda)^2 \tag{14}$$

die Vielfachheit von A um mindestens $x^{(\mathfrak{Z})}$ größer ist als die von $A^{p^{\alpha-1}}$.

4. Läßt man S alle Elemente eines Komplexes $\mathfrak{x}_\nu^{(\mathfrak{Z})}$ durchlaufen, so liegt von den Elementen $S^{-1}A$ in jeder der $p^{\beta-\lambda}$ Elementarspuren

$$\mathfrak{z}_1, \mathfrak{z}_2, \cdots, \mathfrak{z}_{p^{\beta-\lambda}} \tag{15}$$

der Klasse $\mathfrak{Z}(\lambda)$ genau eins.

Beweis: S_1 und S_2 seien zwei Elemente aus $\mathfrak{x}_\nu^{(\mathfrak{Z})}$. Nehmen wir an, daß die Elemente $T_1 = S_1^{-1}A$ und $T_2 = S_2^{-1}A$ der gleichen Elementarspur der Reihe (15) angehören, so können wir setzen $T_2 = T_1^m$. Außerdem ist $S_2 = S_1^l$. Daher wird $S_1^{-l}A = S_1^{-m}A^m$, also

$$S_1^{m-l} = A^{m-1}. \tag{16}$$

Die Ordnung der $\mathfrak{B}$-Komponente von S_1 ist $p^{\beta-\lambda}$. Da die $\mathfrak{B}$-Komponente auf der rechten Seite von (16) E ist, muß $m - l$ durch $p^{\beta-\lambda}$ teilbar sein. Vergleicht man in (16) die höchsten Potenzen von p, welche in den Exponenten der $\mathfrak{A}$-Komponenten aufgehen, so ergibt sich weiter, daß $m - 1$ durch $p^{\beta-\lambda}$ teilbar sein muß. Aus $T_2 = T_1^m$ folgt dann aber $T_2 = T_1$; denn T_1 gehört zur Klasse $\mathfrak{Z}(\lambda)$ und hat daher die Ordnung $p^{\beta-\lambda}$. $T_1 = T_2$ ergibt weiter $S_1 = S_2$. Folglich liegt in jeder Elementarspur (15) höchstens ein Element $S^{-1}A$ mit S aus $\mathfrak{x}_\nu^{(\mathfrak{Z})}$. Bezeichnen wir andrerseits mit $\mathfrak{X}_1(\lambda)$ die Gesamtheit derjenigen Elemente aus $\mathfrak{X}(\lambda)$, bei welchen der Exponent der $\mathfrak{A}$-Komponente die Form $kp + 1$ hat, so hat jedes Element Z einer beliebigen Elementarspur $\mathfrak{z}_\tau$ der Reihe (15) die Gestalt $Z = S^{-1}A$ mit einem passenden Element S aus $\mathfrak{X}_1(\lambda)$. Läßt man Z alle Elemente von $\mathfrak{z}_\tau$ durchlaufen, so müssen, wie wir erkannt haben, die zugehörigen Elemente S alle in voneinander verschiedenen elementaren Hauptspuren von $\mathfrak{X}_1(\lambda)$ enthalten sein. Da nun aber $\mathfrak{X}_1(\lambda)$ nur gerade ebenso viele Hauptspuren enthält wie $\mathfrak{z}_\tau$ Elemente, nämlich $\varphi(p^{\beta-\lambda})$, so muß in jeder dieser Hauptspuren gerade eins unserer Elemente S liegen.

Damit ist unsere Behauptung bewiesen. Gleichzeitig hat sich ergeben, daß der Teilkomplex $\mathfrak{x}_\nu^{(3)}$ von $\mathfrak{x}_\nu'$ $p^{\beta-\lambda}$ Elemente enthält. $\mathfrak{x}_\nu^{(\mathfrak{Y})}$ umfaßt daher die übrigen $p^{\alpha-1} - p^{\beta-\lambda}$ Elemente von $\mathfrak{x}_\nu'$.

5. In jedem der Komplexe $\mathfrak{x}_\nu^{(3)}$ sind $p^{\beta-\lambda}$ Elemente enthalten. Folglich ist $x^{(3)} = u p^{\beta-\lambda}$.

Für die Anzahl w der in $\mathfrak{Z}^*(\lambda)$ enthaltenen Elementarspuren gilt $w \leqq p^{\beta-\lambda}$. Nach dem in Punkt 4 Gesagten ist die Vielfachheit von A in $2(\mathfrak{x}_1^{(3)} + \cdots + \mathfrak{x}_u^{(3)})\,\mathfrak{Z}^*(\lambda)$ gleich $2wu$.

In $\mathfrak{Z}^*(\lambda)^2$ tritt A nicht auf. Soll daher in (14) die Vielfachheit von A um mindestens $x^{(3)}$ größer sein als die von $A^{p^{\alpha-1}}$, so muß jedenfalls $2wu \geqq x^{(3)} = u p^{\beta-\lambda}$ gelten oder $2w \geqq p^{\beta-\lambda}$.

6. Die Summe $\mathfrak{X}(\lambda) + \mathfrak{Y}(\lambda) + \mathfrak{Z}(\lambda)$ besteht aus vollen Nebengruppen nach $\mathfrak{U}$. Da nach Hilfssatz I $\mathfrak{X}(\lambda)$ und $\mathfrak{Y}(\lambda)$ schon für sich allein diese Eigenschaft haben, so gilt das gleiche auch für $\mathfrak{Z}(\lambda)$. $\mathfrak{Z}(\lambda)$ ist ferner ein rationaler Komplex und enthält $p^{\beta-\lambda}\varphi(p^{\beta-\lambda})$ Elemente. Folglich tritt nach Hilfssatz II in $\mathfrak{Z}(\lambda)^2$ $A^{p^{\alpha-1}}$ in der Vielfachheit $p^{\beta-\lambda}\varphi(p^{\beta-\lambda})$ auf. Setzen wir $\mathfrak{Z}(\lambda) = \mathfrak{Z}^*(\lambda) + \overline{\mathfrak{Z}}(\lambda)$, so wird

$$\mathfrak{Z}(\lambda)^2 = \mathfrak{Z}^*(\lambda)^2 + (\mathfrak{Z}^*(\lambda) + \overline{\mathfrak{Z}}(\lambda))\,\overline{\mathfrak{Z}}(\lambda) + \mathfrak{Z}^*(\lambda)\,\overline{\mathfrak{Z}}(\lambda).$$

Der Komplex $\overline{\mathfrak{Z}}(\lambda)$ enthält dabei $(p^{\beta-\lambda} - w)\,\varphi(p^{\beta-\lambda})$ Elemente. Ist nun $w \geqq \frac{1}{2} p^{\beta-\lambda}$, so kann in jedem der beiden Komplexe $(\mathfrak{Z}^*(\lambda) + \overline{\mathfrak{Z}}(\lambda))\,\overline{\mathfrak{Z}}(\lambda)$ und $\mathfrak{Z}^*(\lambda)\,\overline{\mathfrak{Z}}(\lambda)$ die Vielfachheit von $A^{p^{\alpha-1}}$ höchstens gleich

$$(p^{\beta-\lambda} - w)\,\varphi(p^{\beta-\lambda})$$

sein. Folglich muß $A^{p^{\alpha-1}}$ in $\mathfrak{Z}^*(\lambda)^2$ mindestens in der Vielfachheit

$$p^{\beta-\lambda}\varphi(p^{\beta-\lambda}) - 2(p^{\beta-\lambda} - w)\,\varphi(p^{\beta-\lambda}) = (2w - p^{\beta-\lambda})\,\varphi(p^{\beta-\lambda})$$

auftreten. Daher ist in (14) die Vielfachheit von A um höchstens $d = 2wu - (2w - p^{\beta-\lambda})\,\varphi(p^{\beta-\lambda})$ größer als die von $A^{p^{\alpha-1}}$. Nun ist

$$\begin{aligned} d - x^{(3)} = d - u p^{\beta-\lambda} &= 2wu - (2w - p^{\beta-\lambda})\,\varphi(p^{\beta-\lambda}) - u p^{\beta-\lambda} \\ &= (u - \varphi(p^{\beta-\lambda}))\,(2w - p^{\beta-\lambda}). \end{aligned}$$

Aus $u \leqq \varphi(p^{\beta-1})$, $2w \geqq p^{\beta-\lambda}$ folgt weiter $d \leqq x^{(3)}$. In (14) ist daher die Vielfachheit von A um höchstens $x^{(3)}$ größer als die von $A^{p^{\alpha-1}}$. Folglich gilt stets $v(A) \leqq v(A^{p^{\alpha-1}})$.

7. Da p eine ungerade Primzahl sein sollte, kann nur $2w > p^{\beta-\lambda}$ sein. Aus $d = x^{(3)}$ folgt daher $u = \varphi(p^{\beta-\lambda})$. Dies besagt aber, daß $\mathfrak{X}^*(\lambda)$ bereits sämtliche Elementarspuren der Klasse $\mathfrak{X}(\lambda)$ enthält, also mit der Klasse $\mathfrak{X}(\lambda)$ übereinstimmt. Damit ist unser Hilfssatz bewiesen.

§ 6.

Eine besondere Betrachtung erfordert noch der Fall $p = 2$.

Der Beweis von Hilfssatz IIIa im vorigen Paragraphen läßt sich unmittelbar auf diesen Fall übertragen, wenn man beachtet, daß der Komplex $\mathfrak{U}'$ jetzt nur aus dem Element $A^{2^{\alpha-1}}$ besteht, und daß A in $\mathfrak{X}(\beta)^2$ nicht auftritt.

Auch die Punkte 1 bis 6 des Beweises für Hilfssatz IIIb lassen sich unmittelbar übertragen, wenn man berücksichtigt, daß die dort definierten Komplexe $\mathfrak{x}_\nu''$ und folglich auch $\mathfrak{X}''(\lambda)$ jetzt leer sind. Daher gilt für jeden Komplex $\mathfrak{L}(\lambda)$ auch jetzt noch $v(A) \leqq v\left(A^{2^{\alpha-1}}\right)$.

Ist $\mathfrak{H}$ nicht vom Typ $(2^\alpha, 2^{\alpha-1})$ oder ist $\lambda > 0$, so kann wie früher nur dann $v(A) = v\left(A^{2^{\alpha-1}}\right)$ sein, wenn $\mathfrak{L}(\lambda)$ die ganze Klasse $\mathfrak{X}(\lambda)$ umfaßt.

Beweis: Es kann nur dann $v(A) = v\left(A^{2^{\alpha-1}}\right)$ werden, wenn die Vielfachheit von A in (13) um $x^{(\mathfrak{Y})}$ und in (14) um $x^{(3)}$ größer ist als die von $A^{2^{\alpha-1}}$. Damit dies der Fall ist, muß zunächst $y^* = x^{(\mathfrak{Y})}$ sein. y^* ist daher von Null verschieden. Ferner muß zu jedem Element Y aus $\mathfrak{Y}^*(\lambda)$ das Element $Y^{-1}A$ in $\mathfrak{x}_1^{(\mathfrak{Y})} + \cdots + \mathfrak{x}_u^{(\mathfrak{Y})}$ liegen. Ist nun $\mathfrak{H}$ nicht vom Typ $(2^\alpha, 2^{\alpha-1})$ oder ist $\lambda > 0$, so ist dies nur dann möglich, wenn $\mathfrak{L}(\lambda)$ die ganze Klasse $\mathfrak{X}(\lambda)$ enthält:

Es sei $\mathfrak{y}$ eine Elementarspur aus $\mathfrak{Y}^*(\lambda)$, etwa die Spur des Elementes $A^{2^\varkappa}B^{l\,2^\lambda}$. Sind dann

$$\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_m \tag{17}$$

sämtliche $m = \varphi(2^{\varkappa-\lambda})$ Elementarspuren der Klasse $\mathfrak{X}(\lambda)$, so kann man zu jeder vorgeschriebenen Spur $\mathfrak{x}_\mu$ dieser Reihe in $\mathfrak{y}$ ein Element Y derart bestimmen, daß $Y^{-1}A$ in $\mathfrak{x}_\mu$ enthalten ist. Hieraus folgt, daß in (13) die Vielfachheit von A nur dann um $x^{(\mathfrak{Y})}$ größer sein kann als die von $A^{2^{\alpha-1}}$, wenn $\mathfrak{X}^*(\lambda) = \mathfrak{X}(\lambda)$ ist.

$\mathfrak{x}_\mu$ sei die Spur des Elementes $AB^{k\,2^\lambda}$. Erfüllen die beiden Zahlen c und d die Bedingungen

$$c \equiv \frac{k}{k\,2^\varkappa - l}, \qquad d \equiv \frac{k\,2^\varkappa - l}{l} \pmod{2^\alpha},$$

so ist $Y = \left(A^{2^\varkappa}B^{l\,2^\lambda}\right)^c$ in $\mathfrak{y}$ enthalten, weil k eine ungerade Zahl ist. Ferner ist $(Y^{-1}A)^{-d} = AB^{k\,2^\lambda}$. Da l eine ungerade Zahl und $\varkappa > 0$ ist, so ist auch d ungerade, und $Y^{-1}A = \left(AB^{k\,2^\lambda}\right)^d$ ist in $\mathfrak{x}_\mu$ enthalten.

Damit ist unsere Behauptung bewiesen.

Schließen wir zunächst die Gruppen vom Typ $(2^\alpha, 2^{\alpha-1})$ aus, so gelten die Hilfssätze IIIa und IIIb unbeschränkt. Folglich läßt sich

der Beweis von § 4 auf unseren Fall übertragen. Man beachte, daß die dort definierten Komplexe $\mathfrak{X}''(\lambda)$ jetzt leer sind.

Auch auf die Gruppen vom Typ $(2^\alpha, 2^{\alpha-1})$ lassen sich die Betrachtungen aus § 4 anwenden, wenn es bei der Einteilung (8) einen von E verschiedenen Komplex gibt, welcher kein Element der Klasse $\mathfrak{X}(0)$ enthält. Man beachte jedoch, daß die letzte Bemerkung in Punkt 4 des Beweises von § 4 für den Fall $\alpha = 2$, also $\beta = 1$, nicht mehr richtig ist. Die zugehörige Gruppe $\mathfrak{H}$ vom Typ (4, 2) läßt sich direkt behandeln.

Wir können daher annehmen, daß die Elemente der Klasse $\mathfrak{X}(0)$ auf alle von E verschiedenen Komplexe verteilt seien.

Es ist jetzt möglich, daß für einen Komplex $\mathfrak{L}(0)$ $v(A) = v(A^{2^{\alpha-1}})$ gilt, ohne daß $\mathfrak{L}(0)$ die ganze Klasse $\mathfrak{X}(0)$ enthält. Damit $v(A) = v(A^{2^{\alpha-1}})$ gilt, ist aber auch jetzt noch notwendig, daß in (14) die Vielfachheit von A um $x^{(3)}$ größer ist als die von $A^{2^{\alpha-1}}$. Umfaßt $\mathfrak{L}(0)$ noch nicht die ganze Klasse $\mathfrak{X}(0)$, so muß, wie aus dem Beweis von Hilfssatz IIIb folgt, $w = 2^{\beta-1}$ sein. $\mathfrak{Z}^*(0)$ enthält dann also genau die Hälfte aller Elemente aus $\mathfrak{Z}(0)$. Diese Elemente müssen jedoch so ausgewählt sein, daß in $\mathfrak{Z}^*(0)^2$ das Element $A^{2^{\alpha-1}}$ nicht auftritt. Von je zwei Elementen Z und $ZA^{2^{\alpha-1}}$ aus $\mathfrak{Z}(0)$ darf daher immer nur das eine in $\mathfrak{Z}^*(0)$ enthalten sein. Denn andernfalls würde $\mathfrak{Z}^*(0)$ als rationaler Komplex auch das Element Z^{-1} enthalten, und in $\mathfrak{Z}^*(0)^2$ würde daher doch das Element $Z^{-1}ZA^{2^{\alpha-1}} = A^{2^{\alpha-1}}$ vorkommen.

In jedem Komplex $\mathfrak{L}(0)$, für den $v(A) = v(A^{2^{\alpha-1}})$ gelten soll, muß die Hälfte aller Elemente der Klasse $\mathfrak{X}(0)$ enthalten sein. Unserer Annahme nach kommt in jedem von E verschiedenen Komplex der Einteilung (8) ein Teilkomplex $\mathfrak{X}^*(0)$ vor. Daraus folgt, daß die Einteilung (8) außer aus E nur noch aus zwei rationalen Komplexen besteht:

$$\mathfrak{S}_2 = \mathfrak{X}_2(0) + \mathfrak{Z}_2(0) + \mathfrak{C}_2,$$
$$\mathfrak{S}_3 = \mathfrak{X}_3(0) + \mathfrak{Z}_3(0) + \mathfrak{C}_3.$$

Die $\mathfrak{B}$-Komponenten aller Elemente aus $\mathfrak{C}_2$ und $\mathfrak{C}_3$ sind gerade Zahlen. Die Elemente der Klasse $\mathfrak{Z}(0)$ müssen in der oben beschriebenen Weise auf $\mathfrak{Z}_2(0)$ und $\mathfrak{Z}_3(0)$ verteilt sein. Einer der beiden Komplexe, etwa $\mathfrak{S}_3$, enthält alle von E verschiedenen Potenzen von A.

In $\mathfrak{C}_2$ sei $\mathfrak{C}$ die Gesamtheit aller Elemente, bei welchen der Exponent der $\mathfrak{A}$-Komponente eine ungerade Zahl ist. $\mathfrak{C}$ ist leer oder besteht aus vollen Nebengruppen nach $\mathfrak{U}$. Die übrigen Elemente von $\mathfrak{C}_2$ fassen wir, soweit es möglich ist, zu vollen Nebengruppen nach $\mathfrak{U}$

zusammen (d. h. zu Paaren C und $CA^{2^{\alpha-1}}$). Dadurch möge der Komplex $\mathfrak{D}$ entstehen. Die übrigen Elemente von $\mathfrak{D}$ bilden den Komplex $\mathfrak{F}$. ($\mathfrak{D}$ und $\mathfrak{F}$ können auch leer sein.) Jeder der drei Komplexe $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{F}$ ist offenbar rational.

X sei ein beliebiges Element aus $\mathfrak{X}_3(o)$. Wir werden zeigen, daß in $\mathfrak{S}_2{}^2$ das Element $A^{2^{\alpha-1}}$ in größerer Vielfachheit auftritt als das Element X. Daraus folgt, daß auch bei den Gruppen vom Typ $(2^\alpha, 2^{\alpha-1})$ unsere Annahme über die Einteilungen in primäre Komplexe falsch ist.

$\mathfrak{X}_2{}^*(o)$ sei derjenige Teilkomplex von $\mathfrak{X}_2(o)$, in welchem die Elemente die Form $S = XD^{-1}$ haben mit einem Element D aus $\mathfrak{D}$. Dann wird $\mathfrak{X}_2(o) = \mathfrak{X}_2{}^*(o) + \mathfrak{X}_2{}^{**}(o)$ und

$$\mathfrak{S}_2 = \mathfrak{X}_2{}^*(o) + \mathfrak{X}_2{}^{**}(o) + \mathfrak{Z}_2(o) + \mathfrak{C} + \mathfrak{D} + \mathfrak{F}.$$

$\mathfrak{X}_2{}^*(o)$ ist leer oder besteht aus vollen Nebengruppen nach $\mathfrak{U}$; denn $\mathfrak{X}_2(o)$ und $\mathfrak{D}$ bestehen aus vollen Nebengruppen nach $\mathfrak{U}$.

Indem man beachtet, daß bei dem Element X sowohl der Exponent der $\mathfrak{A}$-Komponente als auch der Exponent der $\mathfrak{B}$-Komponente ungerade Zahlen sind, erkennt man leicht, daß in $\mathfrak{S}_2{}^2$ das Element X nur in den Produkten

$$2\,\mathfrak{X}_2{}^*(o)\,\mathfrak{D},\quad 2\,\mathfrak{X}_2{}^{**}(o)\,\mathfrak{F},\quad 2\,\mathfrak{Z}_2(o)\,\mathfrak{C}$$

auftreten kann.

In den Komplexen $\mathfrak{X}_2{}^*(o)$, $\mathfrak{X}_2{}^{**}(o)$, $\mathfrak{D}$, $\mathfrak{C}$ seien der Reihe nach x^*, y^*, d, c Elemente enthalten.

In $2\mathfrak{X}_2{}^*(o)\,\mathfrak{D}$ ist die Vielfachheit von X höchstens gleich der kleineren der beiden Zahlen $2x^*$ und $2d$. Diese Zahl sei $2m$. Die beiden Komplexe $\mathfrak{F}$ und $\mathfrak{Z}_2(o)$ haben die Eigenschaft, daß sie von zwei Elementen R und $RA^{2^{\alpha-1}}$ immer höchstens nur das eine enthalten können. $\mathfrak{X}_2{}^{**}(o)$ und $\mathfrak{C}$ bestehen dagegen aus vollen Nebengruppen nach $\mathfrak{U}$, d. h. aus Paaren T und $TA^{2^{\alpha-1}}$. Daher gibt es höchstens zu jedem zweiten Element aus $\mathfrak{X}_2{}^{**}(o)$ bzw. aus $\mathfrak{C}$ ein solches Element in $\mathfrak{F}$ bzw. in $\mathfrak{Z}_2(o)$, das das Produkt X ergibt. Folglich ist in $2\mathfrak{X}_2{}^{**}(o)\,\mathfrak{F}$ die Vielfachheit von X höchstens x^{**} und in $2\,\mathfrak{Z}_2(o)\,\mathfrak{C}$ höchstens c. In $\mathfrak{S}_2{}^2$ ist daher die Vielfachheit von X höchstens gleich

$$r = 2m + x^{**} + c.$$

$A^{2^{\alpha-1}}$ tritt in $\mathfrak{S}_2{}^2$ in den Teilkomplexen $\mathfrak{X}_2(o)^2$, $\mathfrak{C}^2$ und $\mathfrak{D}^2$ auf, und zwar (nach Hilfssatz I und II) der Reihe nach in der Vielfachheit $x^* + x^{**}$, c und d. Für die Vielfachheit s von $A^{2^{\alpha-1}}$ in $\mathfrak{S}_2{}^2$ gilt daher

$$s = x^* + x^{**} + c + d.$$

Nun ist $x^* + d \geqq 2m$, also jedenfalls $s \geqq r$. Das Gleichheitszeichen kann hier nur dann stehen, wenn $x^* = d$ ist. Damit dann aber wirklich

$r = s$ wird, müßte X in $2\mathfrak{X}_2^*(o)\,\mathfrak{D}$ und in $2\mathfrak{X}_2^{**}(o)\,\mathfrak{F}$ in der Vielfachheit x^* bzw. x^{**} auftreten. Dazu müßte aber zu zwei Elementen S und $SA^{2^{\alpha-1}}$ aus $\mathfrak{X}_2(o)$ stets eins der Elemente XS^{-1} oder $XS^{-1}A^{2^{\alpha-1}}$ in $\mathfrak{D}$ oder in $\mathfrak{F}$ liegen. Da es nun aber auch zwei solche Elemente S und $SA^{2^{\alpha-1}}$ in $\mathfrak{X}_2(o)$ gibt, welche beide die gleiche $\mathfrak{B}$-Komponente haben wie X, so müßte es in $\mathfrak{D}$ oder $\mathfrak{F}$ also auch Elemente geben, deren $\mathfrak{B}$-Komponente E ist, d. h. Potenzen von A. Dies ist jedoch unmöglich, da alle Potenzen von A in $\mathfrak{S}_3$ enthalten sind.

Damit ist auch für $p = 2$ unser Satz bewiesen.

§ 7.

Der zweite Teil unserer in der Einleitung aufgestellten Behauptung folgt aus einem etwas allgemeineren Satz:

Es sei $m > 2$ eine beliebige ganze Zahl. Ist $\mathfrak{H}$ eine reguläre Abelsche Permutationsgruppe des Grades m^2, welche sich als direktes Produkt zweier zyklischer Gruppen der Ordnung m darstellen läßt, so lassen sich stets primitive, einfach transitive Permutationsgruppen $\mathfrak{G}$ des Grades m^2 angeben, welche $\mathfrak{H}$ als Untergruppe enthalten.

Nach den Ergebnissen des § 1 ist dieser Satz als bewiesen anzusehen, wenn wir eine Permutationsgruppe $\mathfrak{G}$ des Grades m^2 angeben können, durch welche $\mathfrak{H}$ in mehr als zwei primäre Komplexe zerfällt, von denen keiner singulär ist.[11])

Es sei $$\mathfrak{H} = \mathfrak{A} \times \mathfrak{B}$$

das direkte Produkt der beiden zyklischen Gruppen

$$\mathfrak{A} = E + A + A^2 + \cdots + A^{m-1} = E + \mathfrak{A}'$$

und $$\mathfrak{B} = E + B + B^2 + \cdots + B^{m-1} = E + \mathfrak{B}'.$$

In der Einteilung

$$\mathfrak{H} = \mathfrak{K}_0 + \mathfrak{K}_1 + \mathfrak{K}_2,$$
$$\mathfrak{K}_0 = E,$$
$$\mathfrak{K}_1 = \mathfrak{A}' + \mathfrak{B}' = A + A^2 + \cdots + A^{m-1} + B + B^2 + \cdots + B^{m-1},$$
$$\mathfrak{K}_2 = \mathfrak{A}'\,\mathfrak{B}' = \sum_{\varrho,\,\sigma=1}^{m-1} A^\varrho B^\sigma$$

ist offenbar kein Komplex singulär. (In $\mathfrak{K}_2$ sind die beiden Elemente AB und AB^2 enthalten, welche die ganze Gruppe $\mathfrak{H}$ erzeugen.)

---

11) Hier zeigt sich, daß es im Falle $m = 2$ keine Gruppe $\mathfrak{G}$ mit der geforderten Eigenschaft gibt. Die Gruppe $\mathfrak{H}$ vom Typ (2, 2) enthält nämlich nur drei von E verschiedene Elemente. Damit ein von E verschiedener Komplex nicht singulär ist, muß er mindestens zwei Elemente enthalten. Daher kann es hier nur einen derartigen Komplex geben.

$\mathfrak{H}$ soll nun derart in eine Gruppe $\mathfrak{G}$ desselben Grades eingebettet werden, daß dabei $\mathfrak{K}_0$, $\mathfrak{K}_1$ und $\mathfrak{K}_2$ als primäre Komplexe entstehen.

Wir führen wie in § 1 die Elemente von $\mathfrak{H}$ als Vertauschungssymbole für die gesuchte Gruppe $\mathfrak{G}$ ein. Diejenige Untergruppe von $\mathfrak{G}$, welche das Einheitselement von $\mathfrak{H}$ ungeändert läßt, bezeichnen wir wieder mit $\mathfrak{G}_1$. Nach dem in § 1 Gesagten muß von der Gruppe $\mathfrak{G}$ nur verlangt werden, daß die von E verschiedenen Elemente von $\mathfrak{H}$ bei den Permutationen von $\mathfrak{G}_1$ in die Transitivitätssysteme $\mathfrak{K}_1$ und $\mathfrak{K}_2$ zerfallen.

$\mathfrak{S}^*$ sei die symmetrische Gruppe in den Symbolen $1, 2, \ldots, m-1$. Jeder Permutation S^* aus $\mathfrak{S}^*$ ordnen wir diejenige Permutation S der Symbole $0, 1, 2, \ldots, m-1$ zu, die 0 ungeändert läßt und $1, 2, \ldots, m-1$ wie S^* vertauscht. Die Gruppe der S heiße $\mathfrak{S}$.

Sind $S_1 = \binom{\varkappa}{\varkappa'}$ und $S_2 = \binom{\varkappa}{\varkappa''}$ $(\varkappa = 0, 1, \ldots, m-1)$ zwei Permutationen aus $\mathfrak{S}$, so möge das Symbol (S_1, S_2) folgende Vertauschung der Elemente von $\mathfrak{H}$ hervorrufen:

$$(A^\varkappa B^\lambda)_{(S_1, S_2)} = A^{\varkappa'} B^{\lambda''} \qquad (\varkappa, \lambda = 0, 1, \ldots, m-1).$$

Ferner definieren wir ein Symbol T, welches die Elemente von $\mathfrak{H}$ in folgender Weise untereinander vertauscht:

$$(A^\varkappa B^\lambda)_T = A^\lambda B^\varkappa \qquad (\varkappa, \lambda = 0, 1, \ldots, m-1).$$

S_3 und S_4 seien Permutationen aus $\mathfrak{S}$. Die Produkte $(S_1, S_2)(S_3, S_4)$, $(S_1, S_2)T$, $T(S_1, S_2)$ werden durch folgende Relationen definiert:

$$(A^\varkappa B^\lambda)_{(S_1, S_2)(S_3, S_4)} = (A^\varkappa B^\lambda)_{(S_1 S_3, S_2 S_4)},$$

$$(A^\varkappa B^\lambda)_{(S_1, S_2)T} = ((A^\varkappa B^\lambda)_{(S_1, S_2)})_T = (A^{\varkappa'} B^{\lambda''})_T = A^{\lambda''} B^{\varkappa'},$$

$$(A^\varkappa B^\lambda)_{T(S_1, S_2)} = ((A^\varkappa B^\lambda)_T)_{(S_1, S_2)} = (A^\lambda B^\varkappa)_{(S_1, S_2)} = A^{\lambda'} B^{\varkappa''}.$$

Es ist $T(S_1, S_2) = (S_2, S_1)T$. Die Gesamtheit der Symbole (S_1, S_2) und $(S_1, S_2)T$ bildet eine Gruppe $\mathfrak{G}^*$ der Ordnung $2[(m-1)!]^2$ von Vertauschungen der Elemente von $\mathfrak{H}$. Alle diese Vertauschungen lassen $E = A^0 B^0$ fest. Die von E verschiedenen Elemente von $\mathfrak{H}$ zerfallen in die Transitivitätssysteme $\mathfrak{K}_1$ und $\mathfrak{K}_2$. Denn eine Potenz von A (geschrieben in der Form $A^\varkappa B^0$) geht durch eine Permutation der Form (S_1, S_2) wieder in eine Potenz von A über und bei Anwendung von T in eine Potenz von B. Bei passender Wahl von S_1 und S_2 läßt sich ferner jedes Produkt $A^\varkappa B^\lambda$ $(\varkappa \neq 0, \lambda \neq 0)$ durch (S_1, S_2) in jedes andere Produkt $A^{\varkappa'} B^{\lambda''}$ $(\varkappa' \neq 0, \lambda'' \neq 0)$ überführen.

$\mathfrak{H}$ fasse man ebenfalls als Gruppe von Permutationen der Elemente $A^{\varkappa}B^{\lambda}$ $(\varkappa, \lambda = 0, 1, \ldots, m-1)$ auf.[12]) Es gilt

$$\mathfrak{G}^*\mathfrak{H} = \mathfrak{H}\mathfrak{G}^*.$$

Beweis: $H = A^aB^b$ bzw. $G^* = (S_1, S_2)$ seien beliebige Elemente aus $\mathfrak{H}$ bzw. $\mathfrak{G}^*$. Das Produkt HG^* ruft folgende Permutation der Elemente $A^{\varkappa}B^{\lambda}$ hervor[13]):

$$(A^{\varkappa}B^{\lambda})_{HG^*} = ((A^{\varkappa}B^{\lambda})_H)_{G^*} = (A^{\varkappa+a}B^{\lambda+b})_{G^*} = A^{(\varkappa+a)'}B^{(\lambda+b)''}.$$

Durch ein Produkt $G_1^*H_1$ $(G_1^* = (S_3, S_4),\ H_1 = A^{a_1}B^{b_1})$ werden $A^{\varkappa}B^{\lambda}$ wie folgt permutiert:

$$(A^{\varkappa}B^{\lambda})_{G_1^*H_1} = ((A^{\varkappa}B^{\lambda})_{G_1^*})_{H_1} = (A^{\varkappa^{III}}B^{\lambda^{IV}})_{H_1} = A^{\varkappa^{III}+a_1}B^{\lambda^{IV}+b_1}.$$

Man kann nun G_1^* und H_1 so bestimmen, daß $G_1^*H_1 = HG^*$ wird, d. h. daß für alle Paare $\varkappa, \lambda = 0, 1, \ldots, m-1$ gilt:

$$\varkappa^{III} + a_1 \equiv (\varkappa + a)', \qquad \lambda^{IV} + b_1 \equiv (\lambda + b)'' \pmod{m}.$$

Für $\varkappa = 0$ wird $a_1 = a'$, für $\lambda = 0$: $b_1 = b'$. Dadurch ist H_1 bestimmt. Indem man für $\varkappa$ bzw. für λ die Werte $1, 2, \ldots, m-1$ einsetzt, werden S_3 bzw. S_4 bestimmt. Da außerdem $A^aB^bT = TA^bB^a$ gilt, so ist jedes Element von $\mathfrak{H}\mathfrak{G}^*$ in $\mathfrak{G}^*\mathfrak{H}$ enthalten. Da überdies die Elemente von $\mathfrak{H}\mathfrak{G}^*$ alle voneinander verschieden sind, folgt $\mathfrak{H}\mathfrak{G}^* = \mathfrak{G}^*\mathfrak{H}$.

Daher ist $\mathfrak{H}\mathfrak{G}^*$ eine Gruppe $\mathfrak{G}$ der Ordnung $2(m!)^2$ von Vertauschungen der Elemente von $\mathfrak{H}$. Diejenige Untergruppe von $\mathfrak{G}$, welche das Einheitselement E von $\mathfrak{H}$ festläßt, ist aber gerade $\mathfrak{G}^*$. $\mathfrak{G}$ ist daher primitiv und einfach transitiv.[14])

Damit ist auch der zweite Teil unseres Satzes bewiesen.

Man erkennt leicht, daß sich unsere letzten Betrachtungen noch verallgemeinern lassen:

$\mathfrak{H}$ sei eine reguläre Abelsche Permutationsgruppe des Grades m^k $(m > 2,\ k \geqq 2)$, welche sich als direktes Produkt der k zyklischen Gruppen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k$ der Ordnung m darstellen läßt. Auch dann gibt es primitive Permutationsgruppen $\mathfrak{G}$ desselben Grades, welche $\mathfrak{H}$ als Untergruppe enthalten und nicht zweifach transitiv sind.

---

12) Man beachte (1) in § 1.

13) Im folgenden sind die Exponenten nötigenfalls mod m zu reduzieren, um $\mathfrak{G}^*$ anwenden zu können.

14) Durch die in der Einleitung genannte Arbeit von Frl. Manning bin ich darauf aufmerksam gemacht worden, daß diese Gruppen $\mathfrak{G}$ schon früher von Herrn W. A. Manning in anderem Zusammenhang behandelt worden sind: *On Primitive Groups of Class Ten.* (American Journ. of Math. Vol. 28 (1906), S. 226—236.)

Um das zu beweisen, geben wir wieder eine Einteilung von $\mathfrak{H}$ in mehr als zwei nicht-singuläre Komplexe an und betten $\mathfrak{H}$ so in eine Gruppe $\mathfrak{G}$ ein, daß diese Komplexe als primäre Komplexe entstehen.

Es sei $$\mathfrak{A}_\varkappa = E + \mathfrak{A}_\varkappa' \qquad (\varkappa = 1, 2, \ldots, k).$$

Von den Komplexen

$$\begin{aligned}
\mathfrak{K}_0 &= E \\
\mathfrak{K}_1 &= \mathfrak{A}_1' + \mathfrak{A}_2' + \cdots + \mathfrak{A}_k' \\
\mathfrak{K}_2 &= \sum_{\varrho<\sigma} \mathfrak{A}_\varrho' \mathfrak{A}_\sigma' \\
\mathfrak{K}_3 &= \sum_{\varrho<\sigma<\tau} \mathfrak{A}_\varrho' \mathfrak{A}_\sigma' \mathfrak{A}_\tau' \\
&\cdots\cdots\cdots \\
\mathfrak{K}_k &= \mathfrak{A}_1' \mathfrak{A}_2' \ldots \mathfrak{A}_k'
\end{aligned}$$

ist, wie man leicht erkennt, keiner singulär, und jedes Element von $\mathfrak{H}$ kommt genau in einem derselben vor. Die Gruppe $\mathfrak{S}$ sei wie oben definiert. Sind

$$S_\varkappa = \begin{pmatrix} \nu \\ \nu^{(\varkappa)} \end{pmatrix} \qquad (\nu = 0, 1, \ldots, m-1;\ \varkappa = 1, 2, \ldots, k)$$

k Permutationen von $\mathfrak{S}$, so soll das Symbol $(S_1, S_2, \ldots, S_k)$ folgende Vertauschung der Elemente von $\mathfrak{H}$ hervorrufen:

$$(A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_k^{\alpha_k})_{(S_1, S_2, \ldots, S_k)} = A_1^{\alpha_1^{(1)}} A_2^{\alpha_2^{(2)}} \ldots A_k^{\alpha_k^{(k)}}.$$

$\mathfrak{T}$ sei die symmetrische Gruppe in k Vertauschungssymbolen. Ist $T = \begin{pmatrix} \varkappa \\ \varkappa' \end{pmatrix}$ eine Permutation aus $\mathfrak{T}$, so definieren wir weiter

$$(A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_k^{\alpha_k})_T = A_1^{\alpha_{1'}} A_2^{\alpha_{2'}} \ldots A_k^{\alpha_{k'}}.$$

Schließlich seien die Produkte $(S_1, S_2, \ldots, S_k)(S_1', S_2', \ldots, S_k')$, $T(S_1, S_2, \ldots, S_k)$, $(S_1, S_2, \ldots, S_k)T$, $T_1 T_2$ durch Zusammensetzung der zugehörigen Permutationen der Elemente von $\mathfrak{H}$ definiert.

Man erkennt leicht, daß die Gesamtheit der Symbole $(S_1, S_2, \ldots, S_k)T$ eine Gruppe $\mathfrak{G}^*$ von Vertauschungen der Elemente von $\mathfrak{H}$ bildet und daß die Gruppe $\mathfrak{G} = \mathfrak{H}\mathfrak{G}^*$ als primäre Komplexe $\mathfrak{K}_0, \mathfrak{K}_1, \ldots, \mathfrak{K}_k$ erzeugt.

Lebenslauf.

Am 21. November 1911 wurde ich, Rudolf Kochendörffer, in Berlin-Pankow geboren als Sohn des Kaufmanns Albert Kochendörffer und seiner Ehefrau Berta, geb. Saß. Vom Herbst 1918 bis zum Herbst 1919 besuchte ich das Dorotheenstädtische Realgymnasium und danach, bis zur Reifeprüfung im Herbst 1930, das Realgymnasium zu Berlin-Pankow. Vom Wintersemester 1930—31 an widmete ich mich dem Studium der Mathematik an der Berliner Universität. Daneben hörte ich naturwissenschaftliche und philosophische Vorlesungen. Meine Universitätslehrer waren die Herren Professoren BAUMGARDT, BIEBERBACH, BRAUER, FEIGL, GEHRCKE, HAMMERSTEIN, N. HARTMANN, HENNING, HETTNER, HOCHSTETTER, W. KÖHLER, v. MISES, NERNST, SCHLENK, E. SCHMIDT, F. J. SCHMIDT, SCHUR, SPRANGER, WEHNELT, WICHMANN und Frau Dr. POLLACZEK-GEIRINGER.

Allen meinen Lehrern bin ich zu großem Dank verpflichtet. Ganz besonders danke ich den Herren Professoren BIEBERBACH, E. SCHMIDT und SCHUR sowie Herrn Dr. BRAUER für die wertvolle Förderung, die ich während meines Studiums durch sie erfahren habe.